Monitor the Performance of Virtual Machines by using Azure Monitor VM Insights

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

Objectives:

- Deploy monitoring for workloads on virtual machines.
- Set up a log analytics workspace, onboard virtual machines to Azure Monitor VM Insights
- Build log queries by using Kusto Query Language.

In this unit, we will:

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

Creating a Log Analytics workspace

Home > Log Analytics workspaces >

Create Log Analytics workspace ...

Basics Tags Review + Create

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-7df27ab4-6a90-4303-85d6-1ebbdda17587

Create new

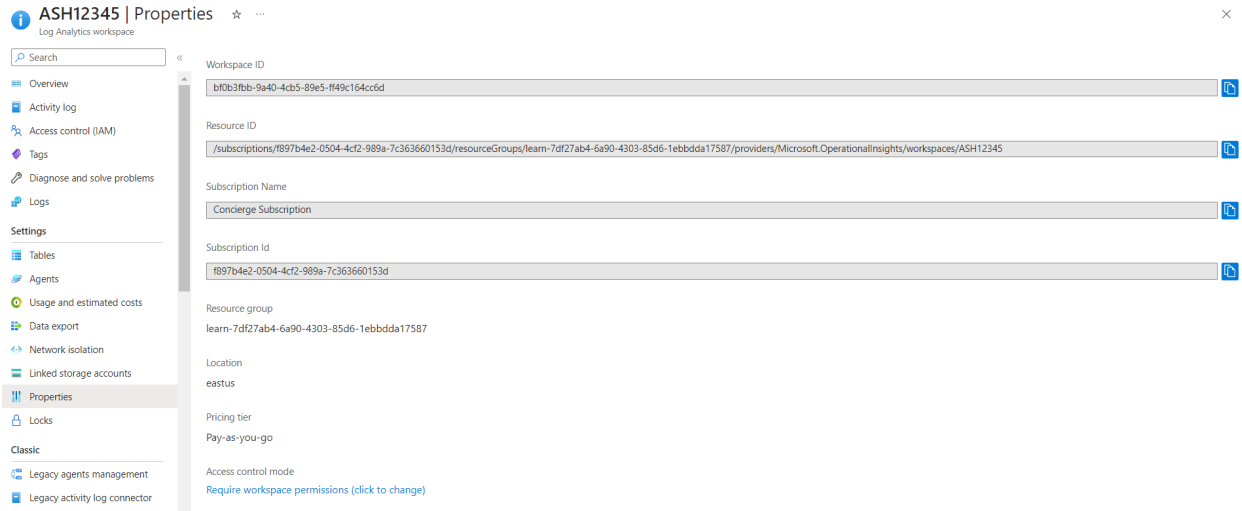
Instance details

Name * ASH12345

Region * East US

Review + Create « Previous Next : Tags >

Look for the access control mode, and select Use resource or workspace permissions. This setting changes the access mode to use the resource-context.



Creating the virtual machines

- **Creating the first virtual machine:**

Run this command in Azure Cloud Shell:

```
az vm create \
  --resource-group learn-7df27ab4-6a90-4303-85d6-1ebbdda17587 \
  --location westus \
  --name SampleVM1 \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys \
  --verbose
```

```
andrijana_sh [ ~ ]$ az vm create \
  --resource-group learn-7df27ab4-6a90-4303-85d6-1ebbdda17587 \
  --location westus \
  --name SampleVM1 \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys \
  --verbose
SSH key files '/home/andrijana_sh/.ssh/id_rsa' and '/home/andrijana_sh/.ssh/id_rsa.pub' have been generated under ~/.ssh to allow SSH access to the VM. If using machines without permanent storage, back up you
keys to a safe location.
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 default public IP used for VM creation will be changed from Basic to Standard in th
future.
Consider using the "Ubuntu2204" alias. On April 30, 2023,the image deployed by the "UbuntuLTS" alias reaches its end of life. The "UbuntuLTS" will be removed with the breaking change release of Fall 2023.
{
  "fqdns": "",
  "id": "/subscriptions/f897b4e2-0504-4cf2-989a-7c363660153d/resourceGroups/learn-7df27ab4-6a90-4303-85d6-1ebbdda17587/providers/Microsoft.Compute/virtualMachines/SampleVM1",
  "location": "westus",
  "macAddress": "00-0D-3A-32-0D-8B",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "20.245.122.0",
  "resourceGroup": "learn-7df27ab4-6a90-4303-85d6-1ebbdda17587",
  "zones": ""
}
```

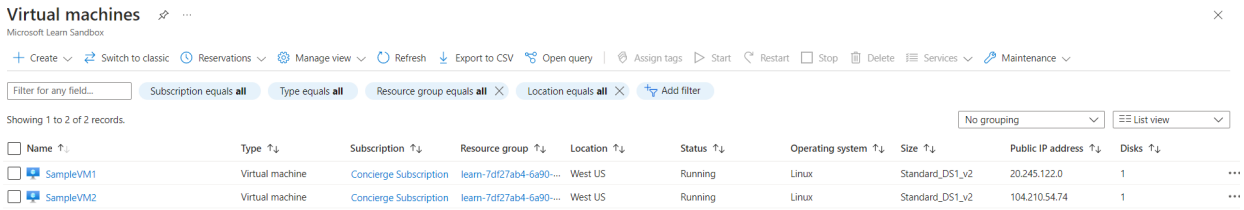
- **Creating the second virtual machine:**

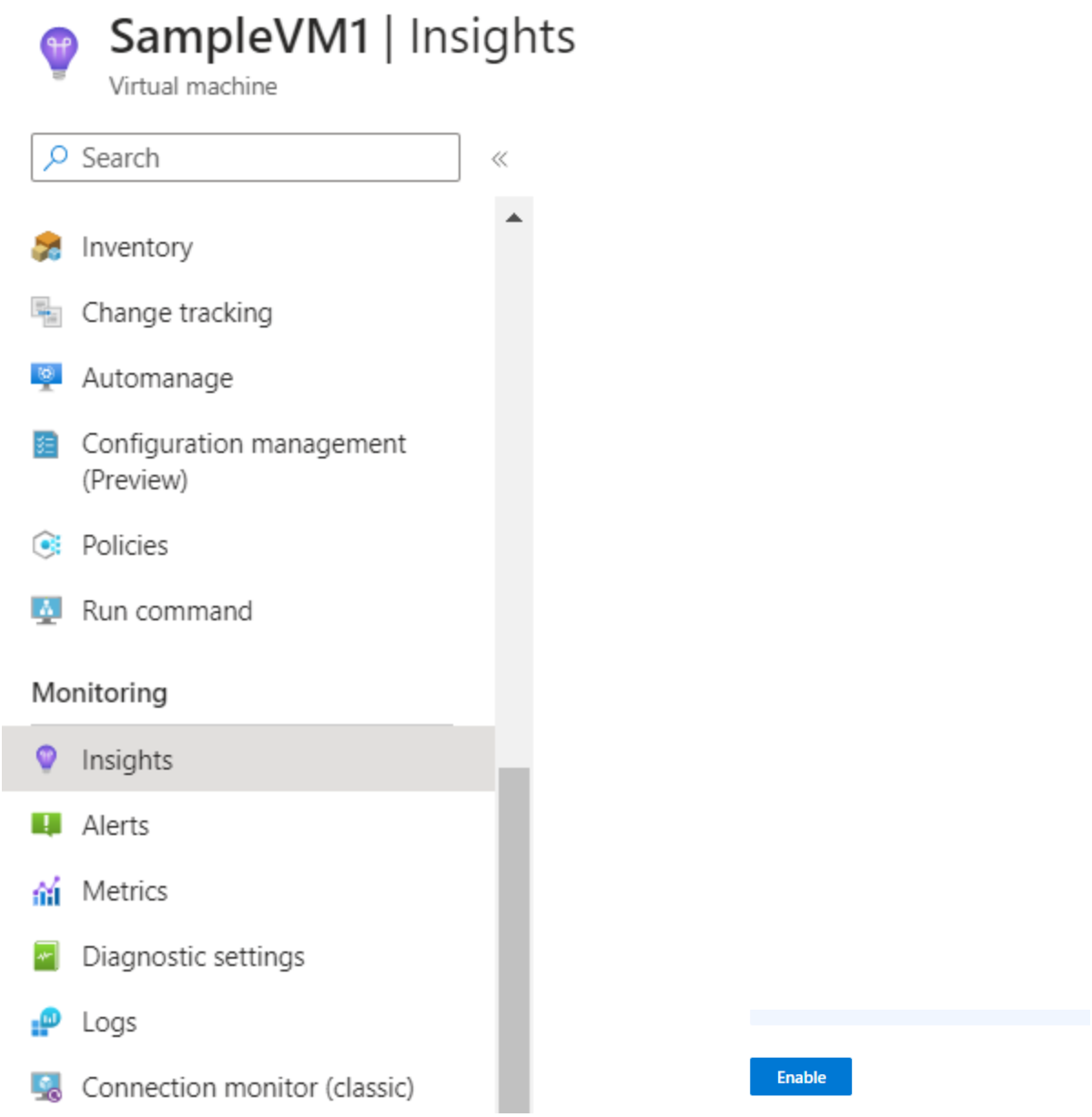
*az vm create *
*--resource-group learn-7df27ab4-6a90-4303-85d6-1ebbdda17587 *
*--location westus *
*--name SampleVM2 *
*--image UbuntuLTS *
*--admin-username azureuser *
*--generate-ssh-keys *
--verbose

```
andrijana_sh [ ~ ]$ az vm create \
  --resource-group learn-7df27ab4-6a90-4303-85d6-1ebbdda17587 \
  --location westus \
  --name SampleVM2 \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys \
  --verbose
Use existing SSH public key file: /home/andrijana_sh/.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 default 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. The "UbuntuLTS" will be removed with the breaking change release of Fall 2023.
{
  "fqdns": "",
  "id": "/subscriptions/f897b4e2-0504-4cf2-989a-7c363660153d/resourceGroups/learn-7df27ab4-6a90-4303-85d6-1ebbdda17587/providers/Microsoft.Compute/virtualMachines/SampleVM2",
  "location": "westus",
  "macAddress": "00-22-48-0A-1A-1E",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.5",
  "publicIpAddress": "104.210.54.74",
  "resourceGroup": "learn-7df27ab4-6a90-4303-85d6-1ebbdda17587",
  "zones": ""
}
```

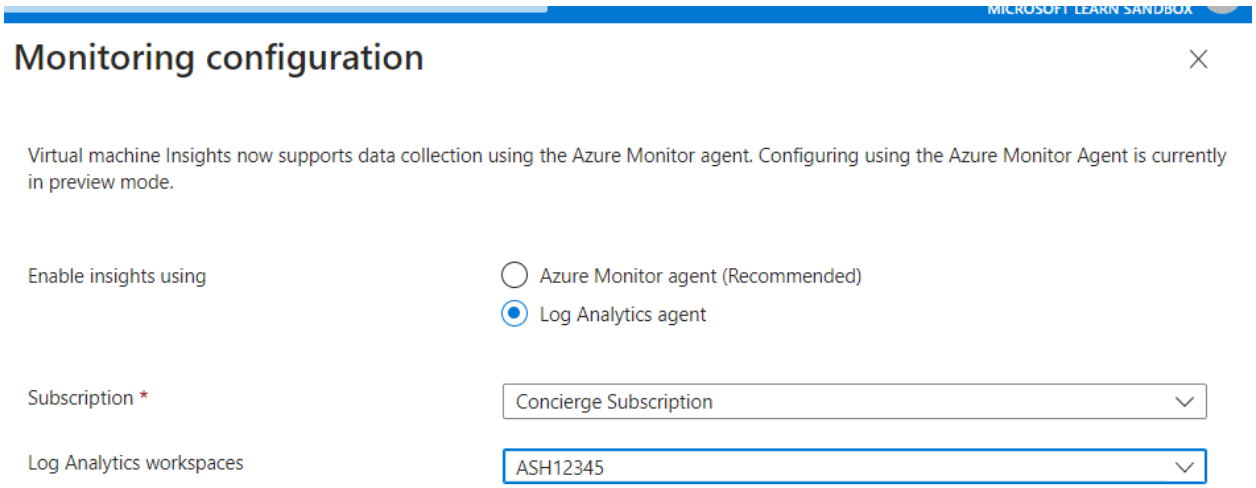
Onboard virtual machines to Azure Monitor VM Insights

Here are the created virtual machines that we will use as samples for this task:

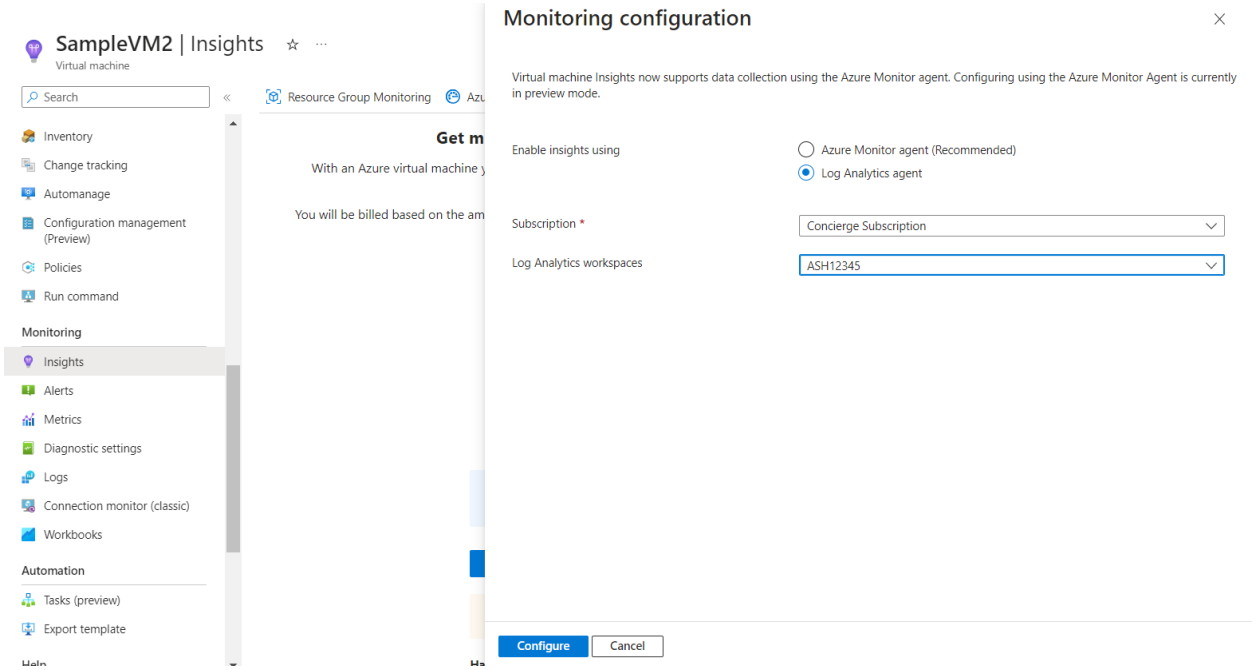



SampleVM1 | Insights
Virtual machine
Search
Inventory
Change tracking
Automanage
Configuration management (Preview)
Policies
Run command
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Logs
Connection monitor (classic)
Enable

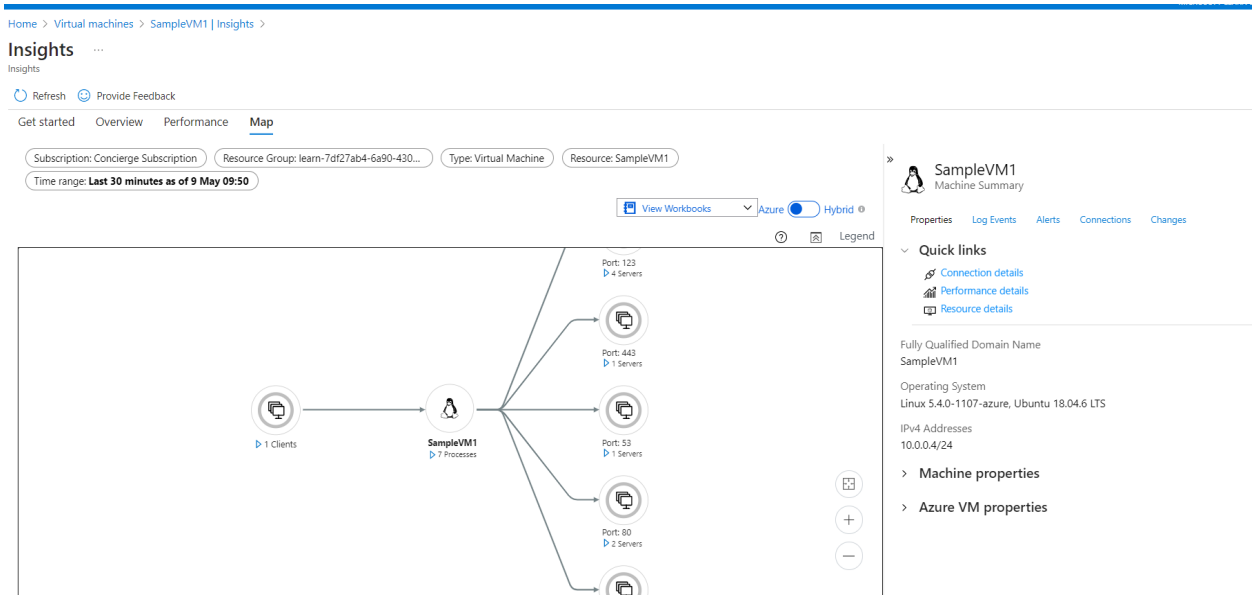
We configure the monitoring by selecting the log analytics workspace we created in the beginning:



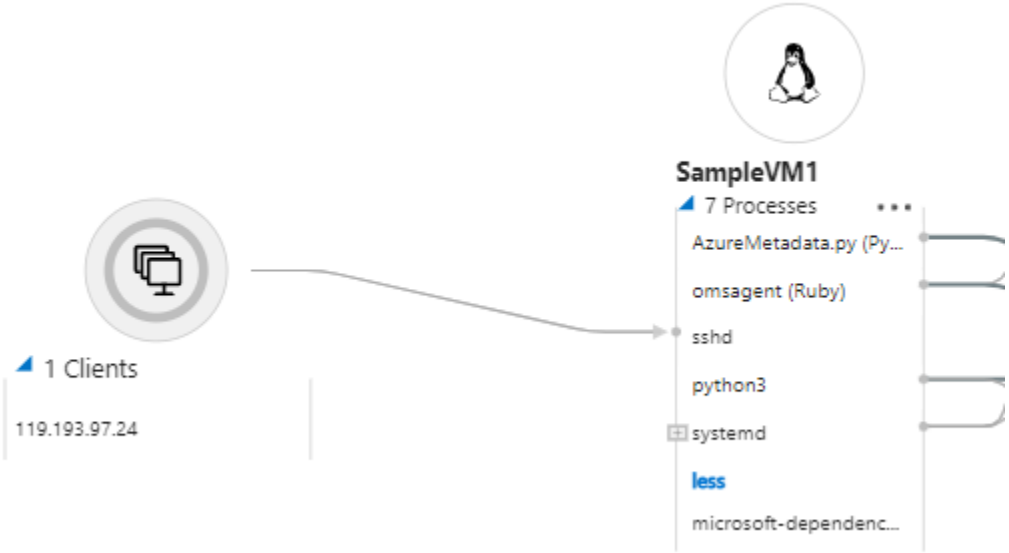
We do the same for the second virtual machine.



We get the monitoring results:



We can review clients, processes, ports, etc.



This is the **Performance Tab**:

Explore the different graphs for:

- Logical Disk Performance
- CPU Utilization
- Available Memory
- Logical Disk IOPS
- Logical Disk MB/s
- Logical Disk Latency (ms)
- Max Logical Disk Used %
- Bytes Sent Rate
- Bytes Received Rate

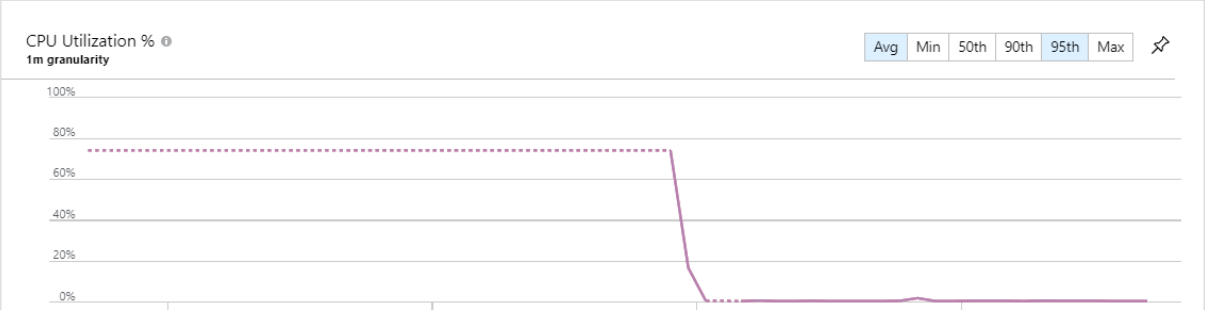
Get started | Performance | Map

Time range: **Last hour as of 9 May 10:10**

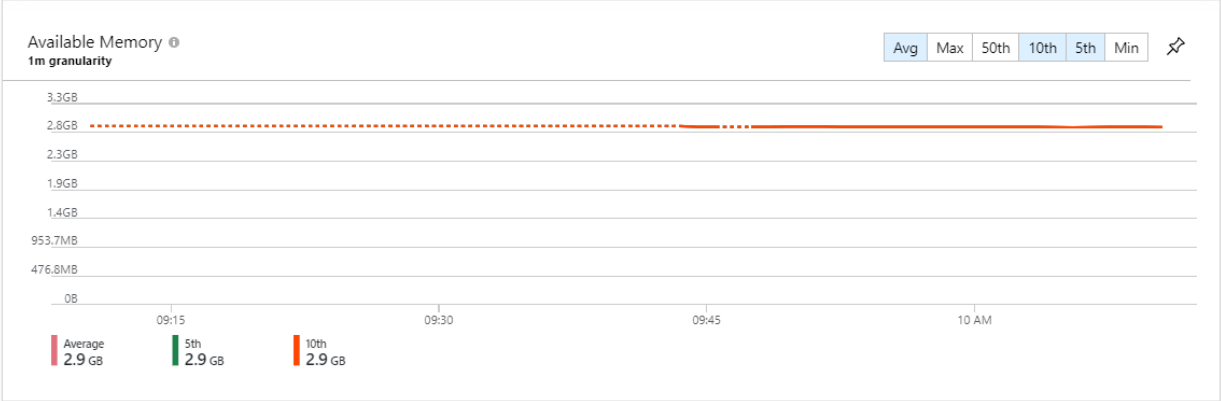
View Workbooks

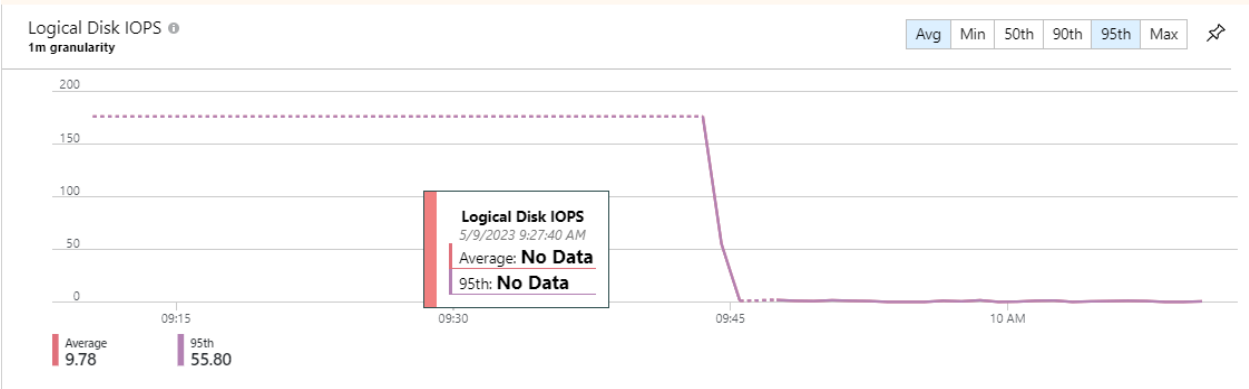
Logical Disk Performance

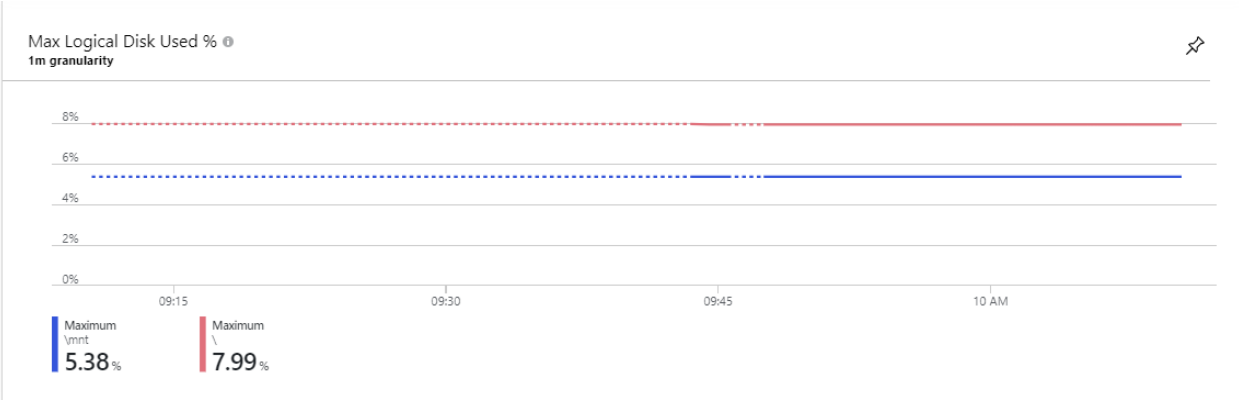
DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPs READ	P95 IOPs WRITE	P95 IOPs TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL
/	28.89	8%	33.21	4.88	55.8	0.72	0.52	2.23
/mnt	6.79	5%	0	0	0	0	0	0
Total	35.69	7%	33.21	4.88	55.8	0.72	0.52	2.23

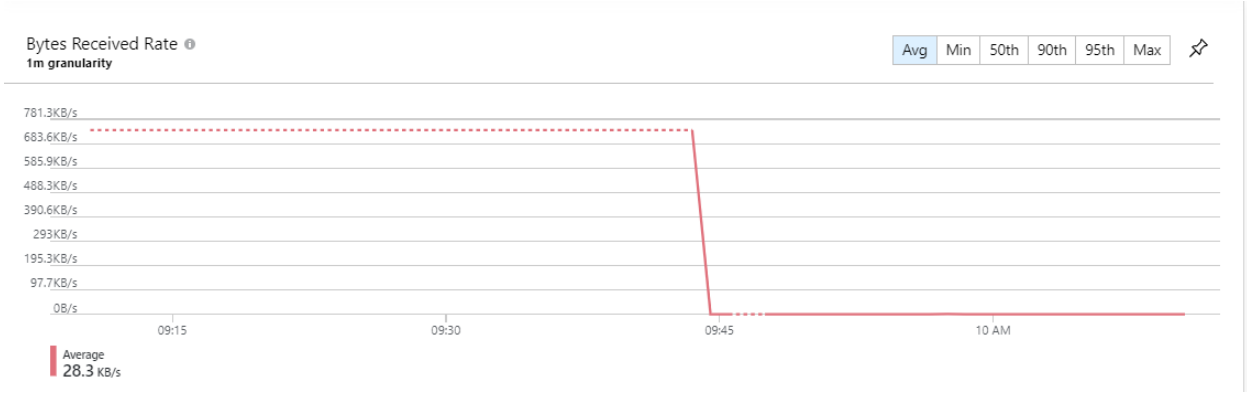



0%
09:15
09:30
09:45
10 AM
Average
4.05 %
95th
16.84 %

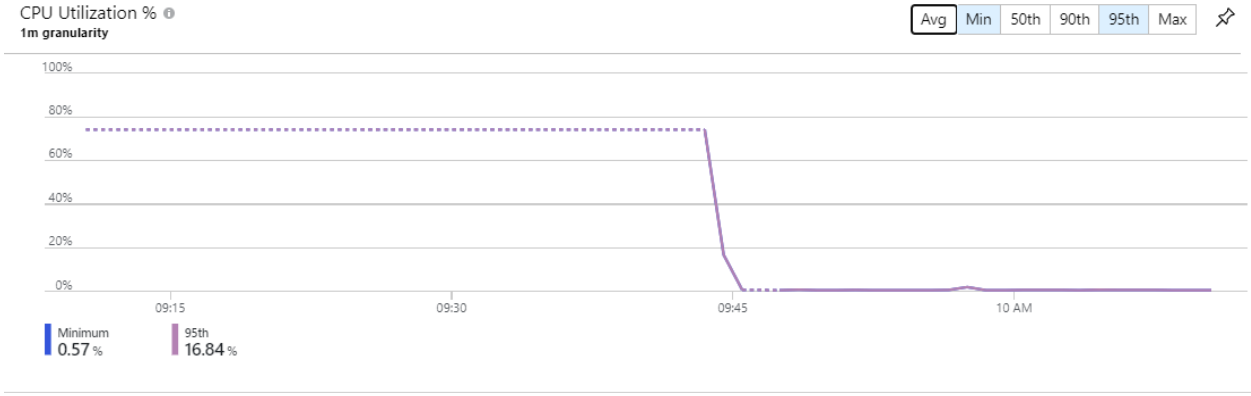

Available Memory
1m granularity
Avg
Max
50th
10th
5th
Min
3.3GB
2.8GB
2.3GB
1.9GB
1.4GB
953.7MB
476.8MB
0B
09:15
09:30
09:45
10 AM
Average
2.9 GB
5th
2.9 GB
10th
2.9 GB


Logical Disk IOPS
1m granularity
Avg
Min
50th
90th
95th
Max
200
150
100
50
0
Logical Disk IOPS
5/9/2023 9:27:40 AM
Average: No Data
95th: No Data
09:15
09:30
09:45
10 AM
Average
9.78
95th
55.80

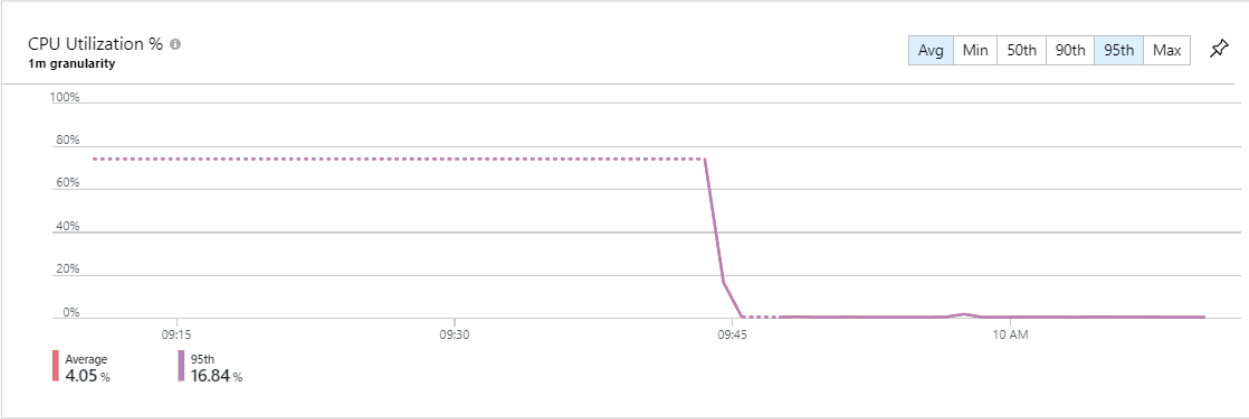

Max Logical Disk Used %
1m granularity
8%
6%
4%
2%
0%
09:15
09:30
09:45
10 AM
Maximum
\mnt
5.38 %
Maximum
\
7.99 %



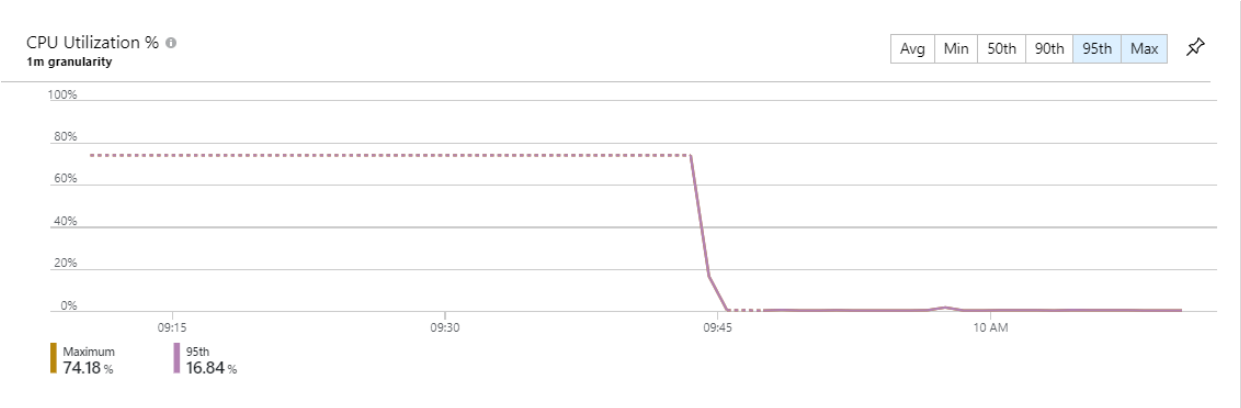
Data from Min CPU utilization



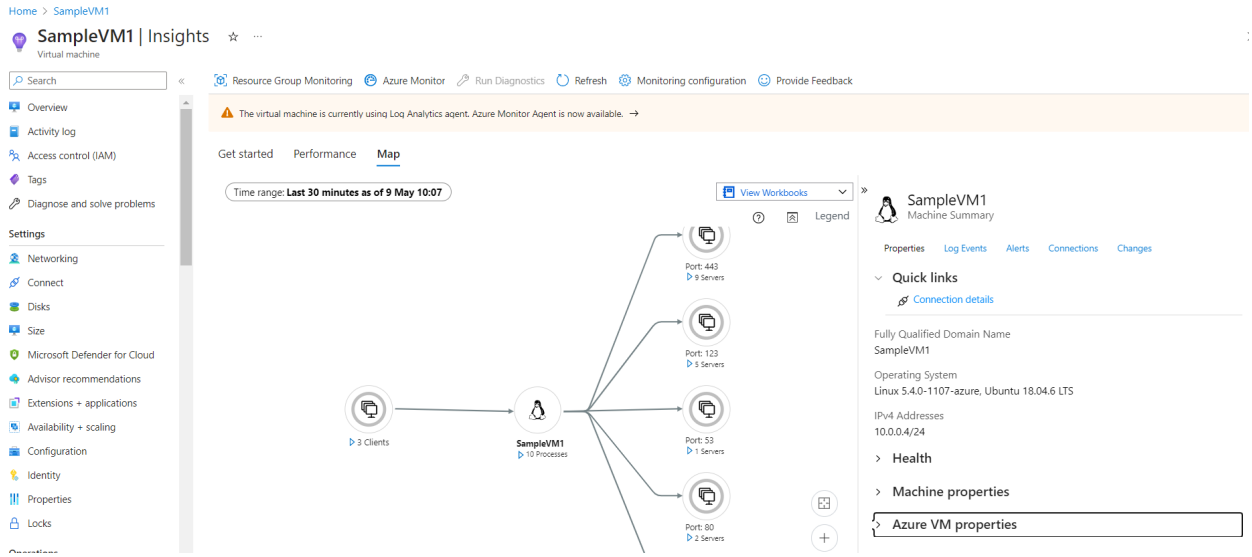
Data for Avg CPU utilization



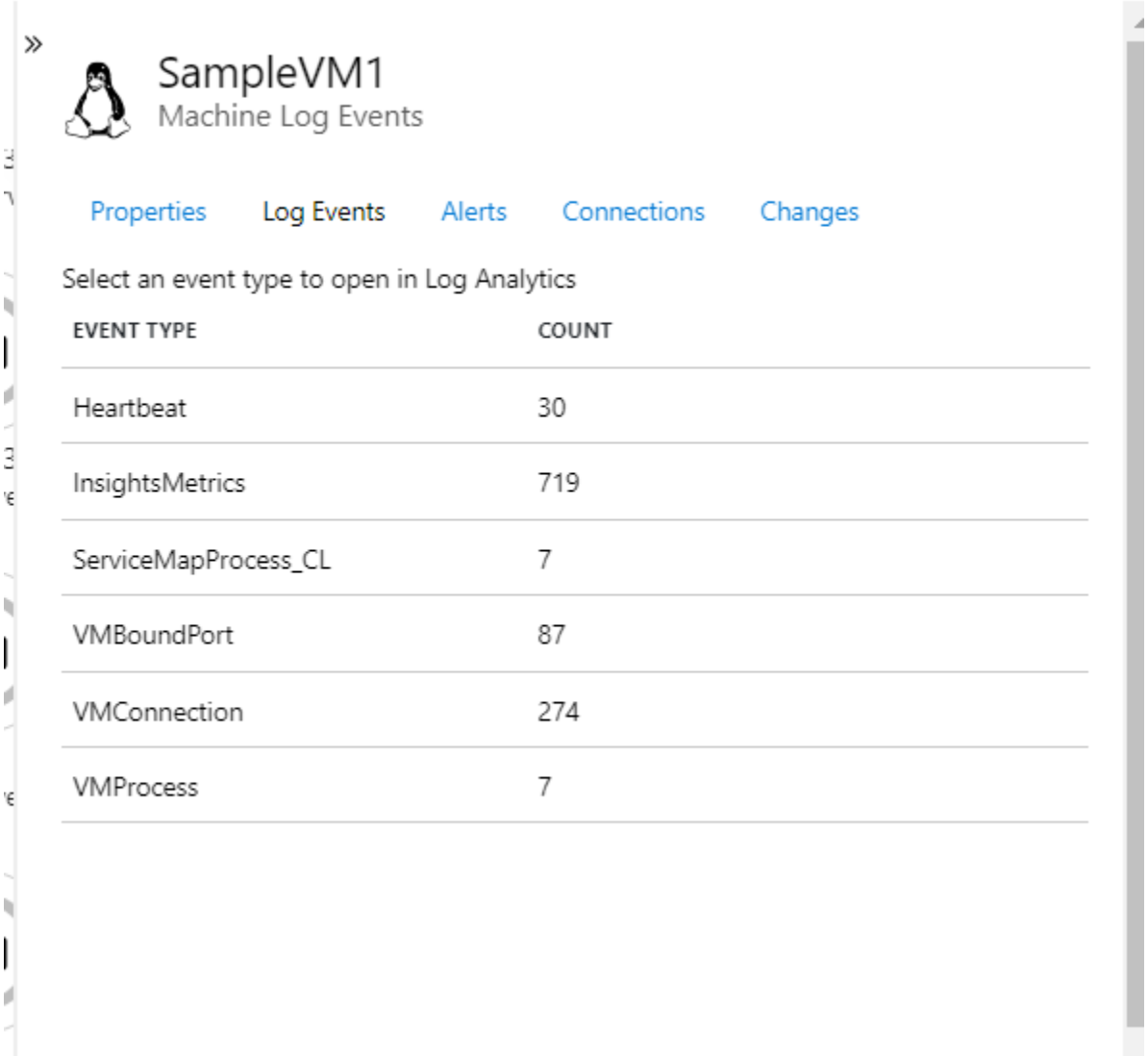
Data for Max CPU utilization



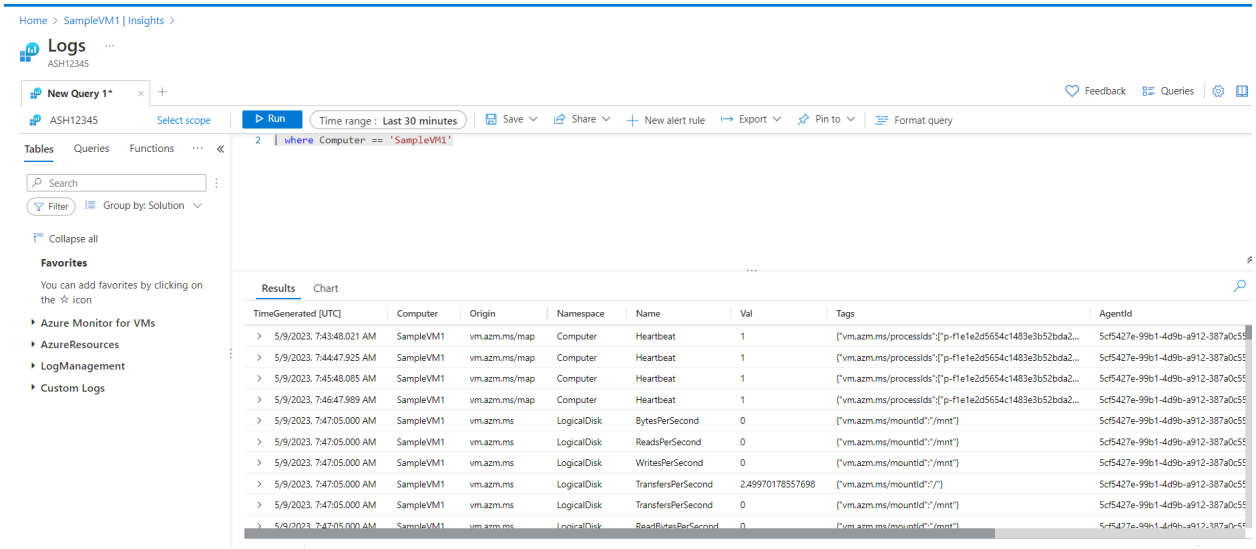
Sample VM1 Insights



Log Events:

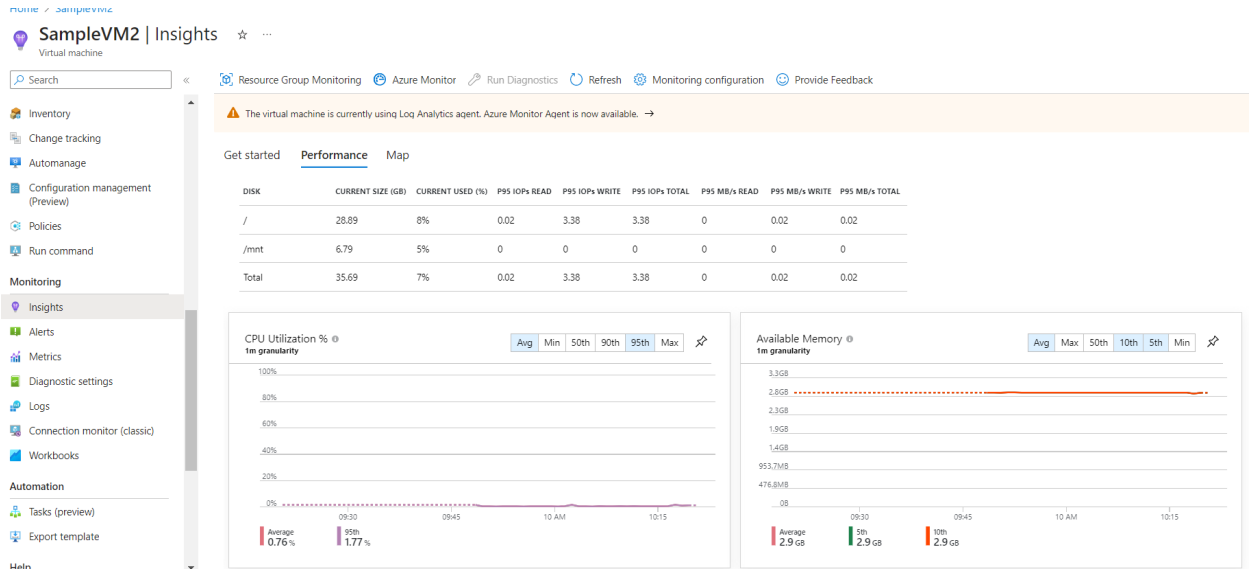

SampleVM1
Machine Log Events
Properties
Log Events
Alerts
Connections
Changes
Select an event type to open in Log Analytics
EVENT TYPE
COUNT
Heartbeat
30
InsightsMetrics
719
ServiceMapProcess_CL
7
VMBoundPort
87
VMConnection
274
VMProcess
7

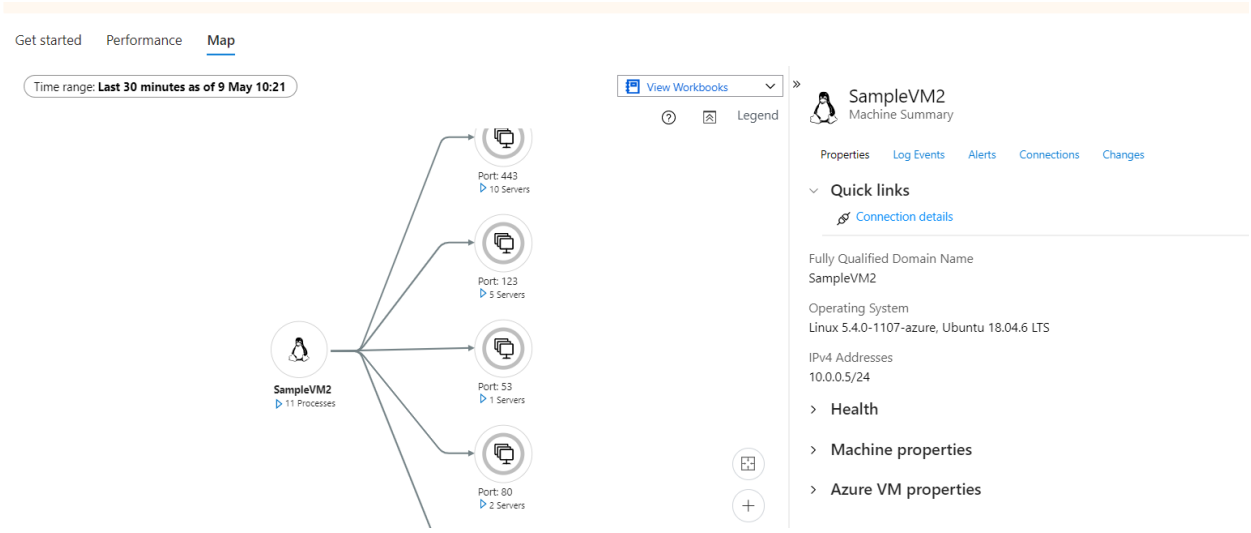
InsightMetrics log:



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

Virtual Machine 2 Insights:





SampleVM2

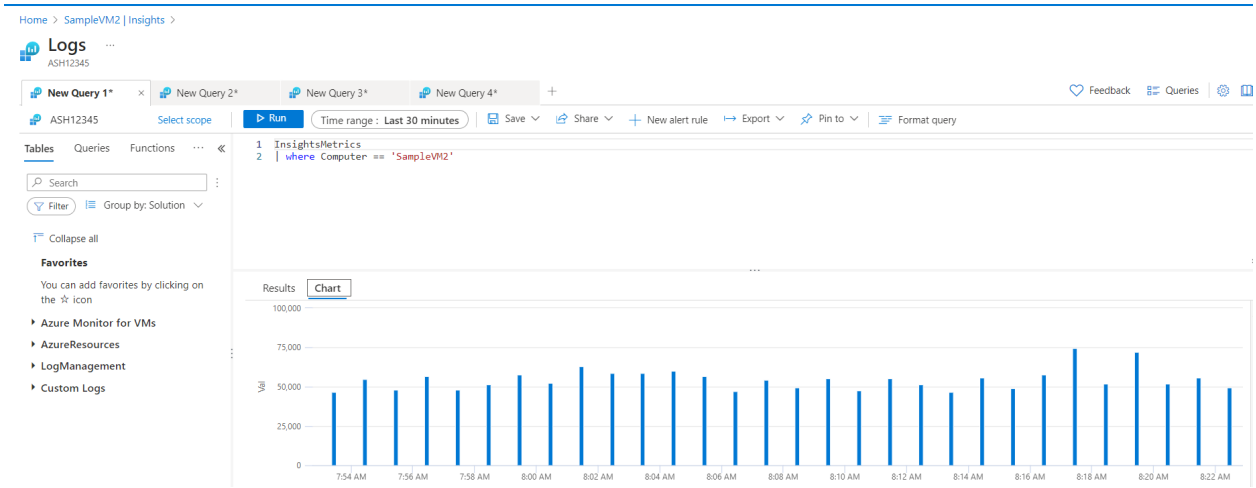
Machine Log Events

Properties | Log Events | Alerts | Connections | Changes

Select an event type to open in Log Analytics

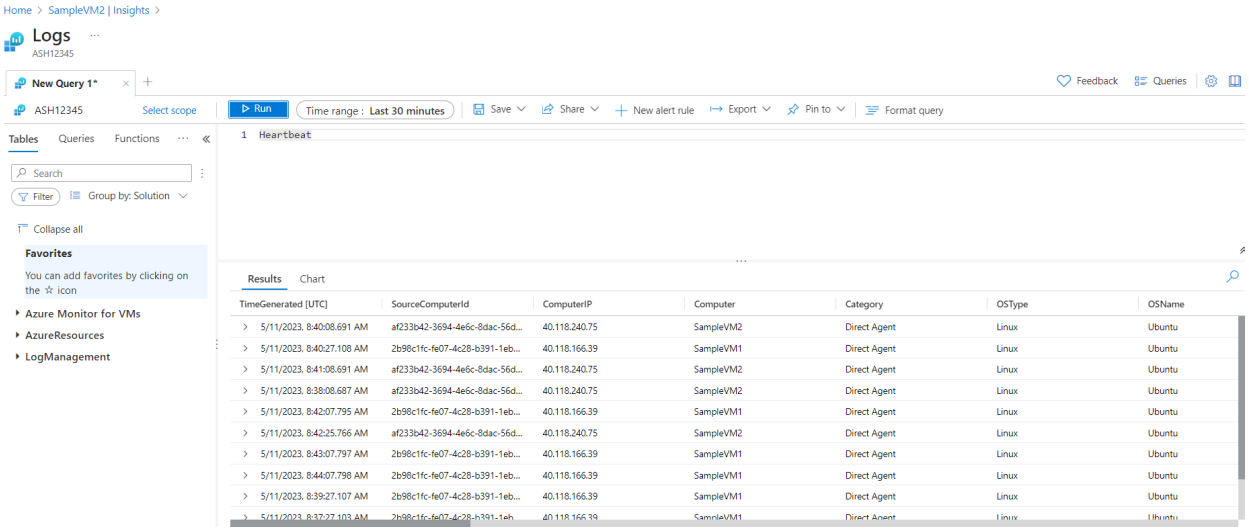
EVENT TYPE	COUNT
Heartbeat	30
InsightsMetrics	719
ServiceMapProcess_CL	4
VMBoundPort	87
VMConnection	265
VMProcess	6

Displaying the results as a chart:

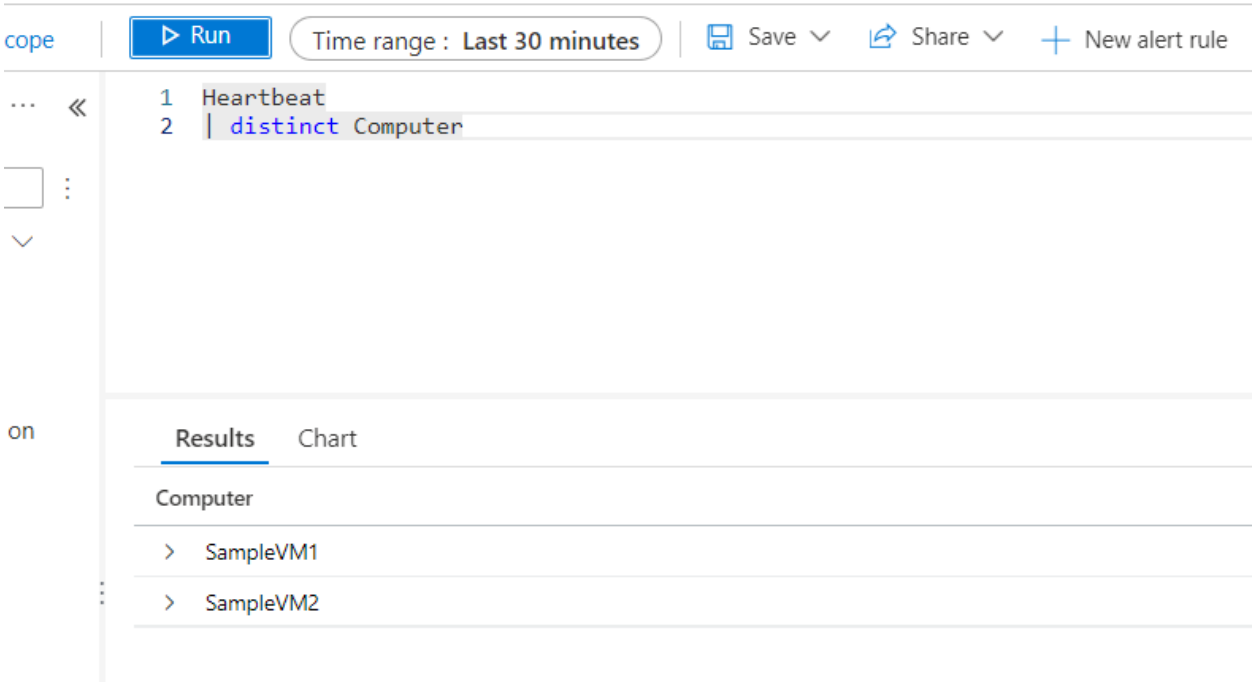


Build log queries by using the Kusto Query Language

- Capturing the information of the Heartbeat table



Using tabular operator ***distinct*** to make sure only the virtual machines we've created are reporting to the Log Analytics workspace



Build log queries

In this unit, we will:

1. Take an existing query, run the query, and analyze the visualizations.
2. Edit the existing query, run the query, and analyze the visualizations.

The query we used:

InsightsMetrics

| where TimeGenerated > ago(1h)

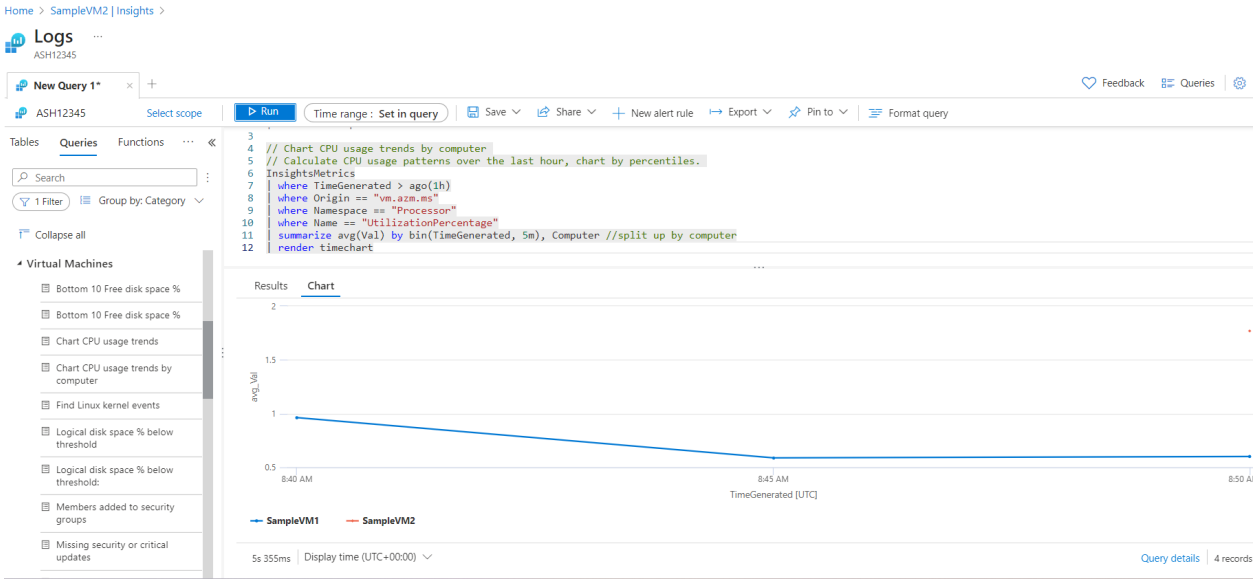
| where Origin == "vm.azm.ms"

| where Namespace == "Processor"

| where Name == "UtilizationPercentage"

| summarize avg(Val) by bin(TimeGenerated, 5m), Computer //split up by computer

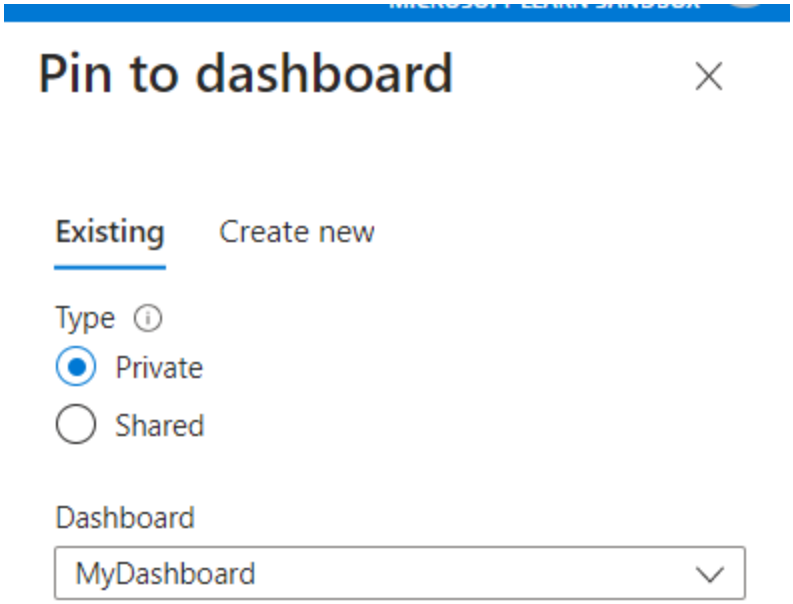
| render timechart



- These results are shown only for SampleVM2 - the second virtual machine

Summarizing the maximum value:

Pinning the results to a dashboard I've created:


Pin to dashboard
Existing
Create new
Type
Private
Shared
Dashboard
MyDashboard