

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

i 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 * ⓘ

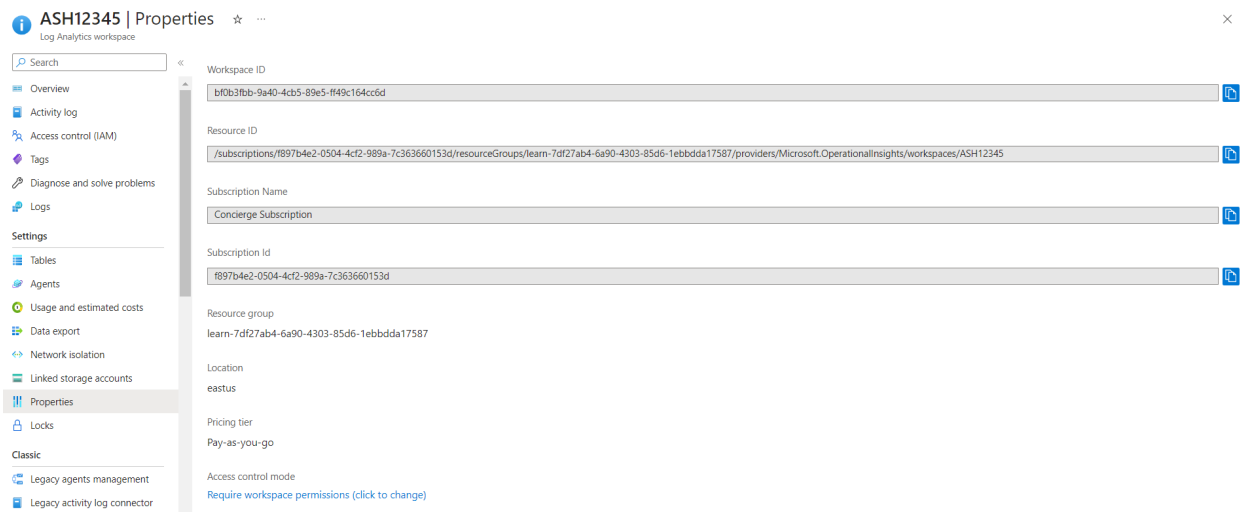
East US

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 your 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 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/SampleVM1",
  "location": "westus",
  "macAddress": "08-00-2A-32-00-8B",
  "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/TLaB
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:

Virtual machines									
Microsoft Learn Sandbox									
+ Create ▾ Switch to classic ⌚ Reservations ▾ ⚙️ Manage view ▾ ↺ Refresh ⬇️ Export to CSV 📄 Open query 🏷️ Assign tags ▶ Start ⌂ Restart ☐ Stop 🗑️ Delete 📋 Services ▾ 🔧 Maintenance ▾									
Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter									
Showing 1 to 2 of 2 records. No grouping List view									
<input type="checkbox"/> Name ↑	Type ↑	Subscription ↑	Resource group ↑	Location ↑	Status ↑	Operating system ↑	Size ↑	Public IP address ↑	Disks ↑
<input type="checkbox"/> SampleVM1	Virtual machine	Concierge Subscription	learn-7df27ab4-6a90-...	West US	Running	Linux	Standard_DS1_v2	20.245.122.0	1
<input type="checkbox"/> SampleVM2	Virtual machine	Concierge Subscription	learn-7df27ab4-6a90-...	West US	Running	Linux	Standard_DS1_v2	104.210.54.74	1



SampleVM1 | Insights

Virtual machine



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:

MICROSOFT LEARN SANDBOX

Monitoring configuration

Virtual machine Insights now supports data collection using the Azure Monitor agent. Configuring using the Azure Monitor Agent is currently in preview mode.

Enable insights using

☐ Azure Monitor agent (Recommended)

☒ Log Analytics agent

Subscription *

Concierge Subscription

Log Analytics workspaces

ASH12345

We do the same for the second virtual machine.

SampleVM2 | Insights

Inventory

Change tracking

Automanage

Configuration management (Preview)

Policies

Run command

Monitoring

Insights

Alerts

Metrics

Diagnostics settings

Logs

Connection monitor (classic)

Workbooks

Automation

Tasks (preview)

Export template

Get m

With an Azure virtual machine y

You will be billed based on the am

Monitoring configuration

Virtual machine Insights now supports data collection using the Azure Monitor agent. Configuring using the Azure Monitor Agent is currently in preview mode.

Enable insights using

☐ Azure Monitor agent (Recommended)

☒ Log Analytics agent

Subscription *

Concierge Subscription

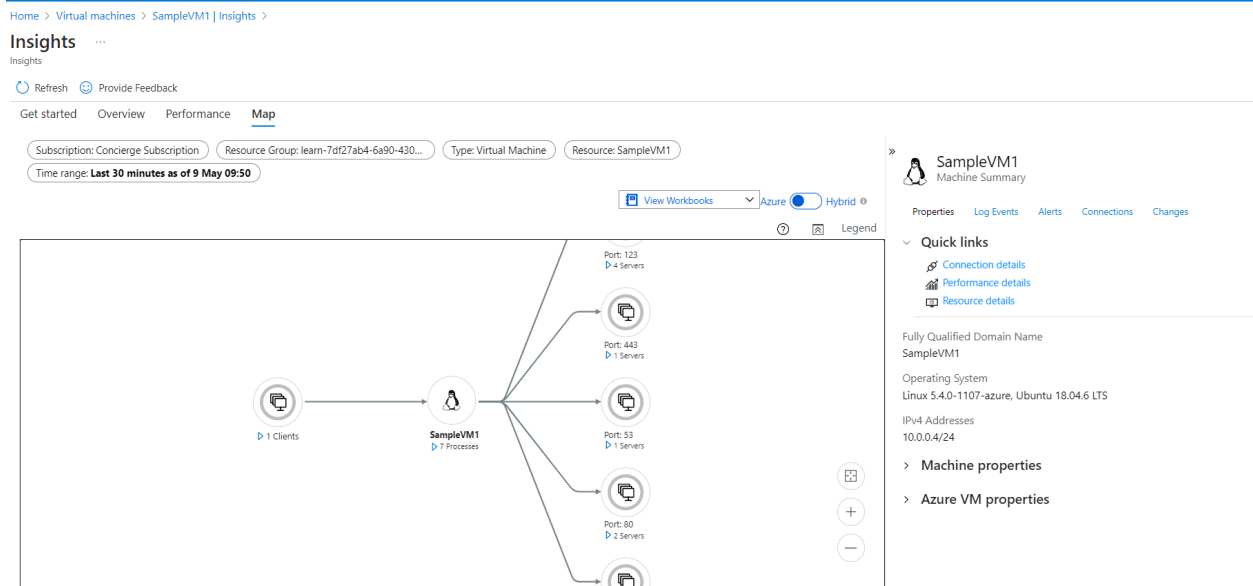
Log Analytics workspaces

ASH12345

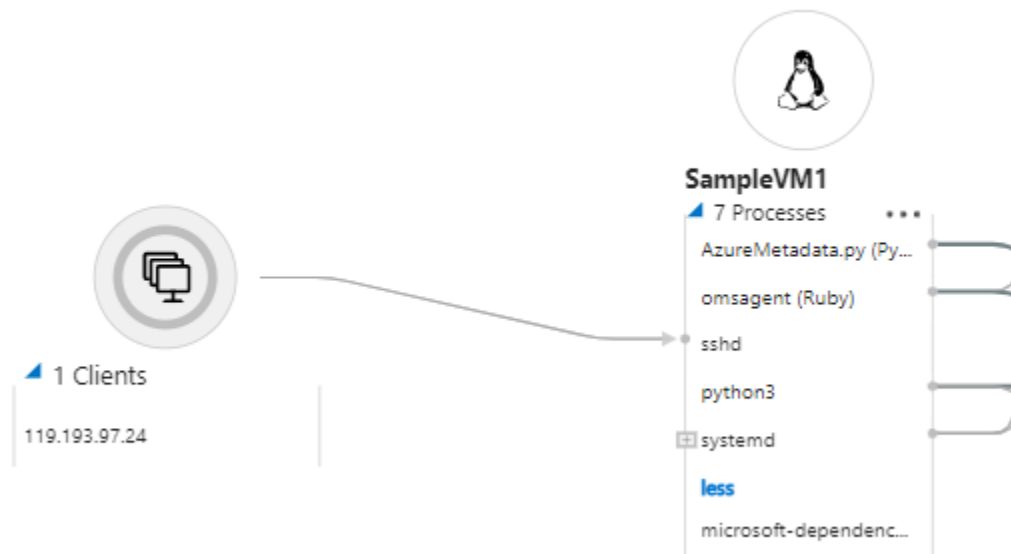
Configure

Cancel

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

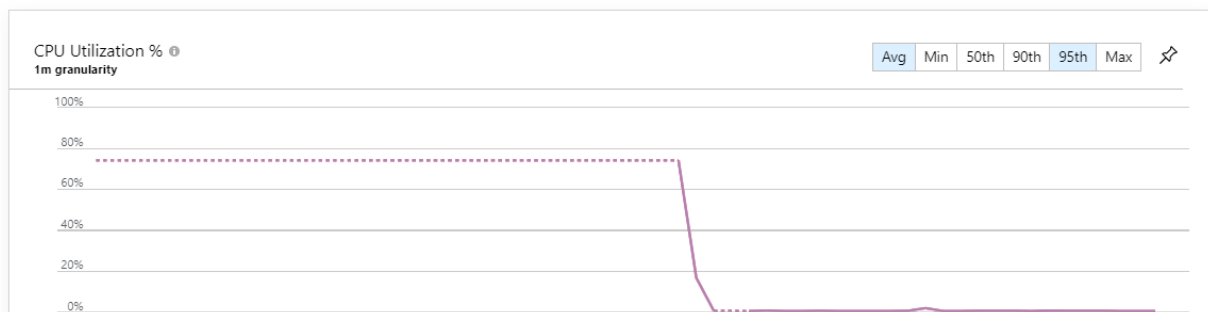
Get started Performance Map

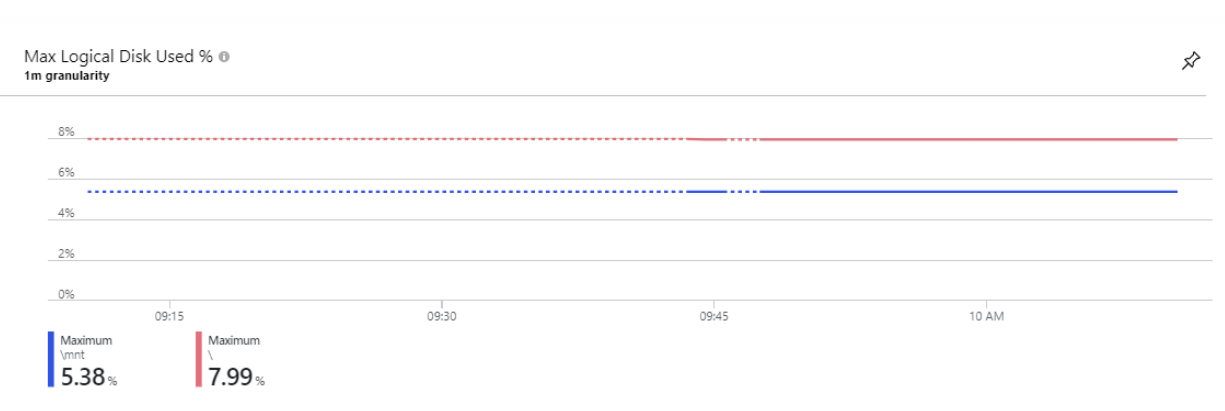
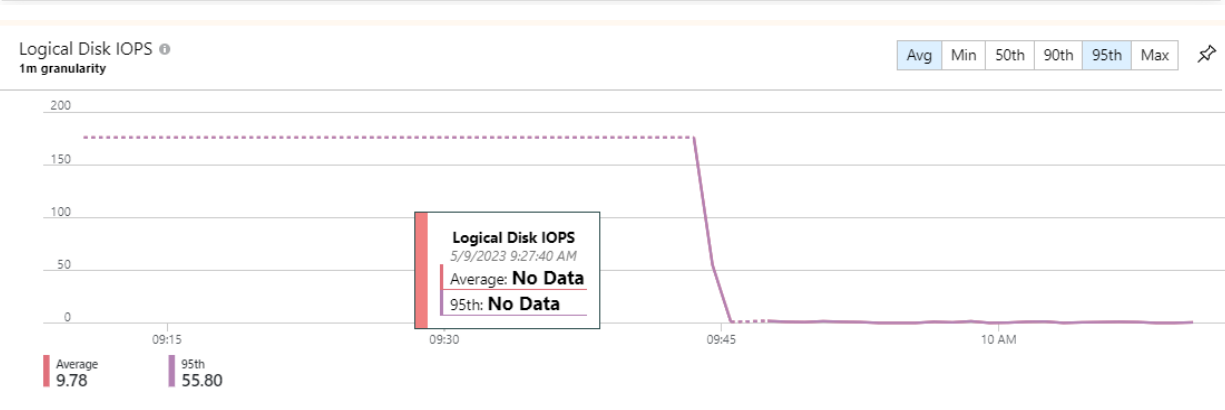
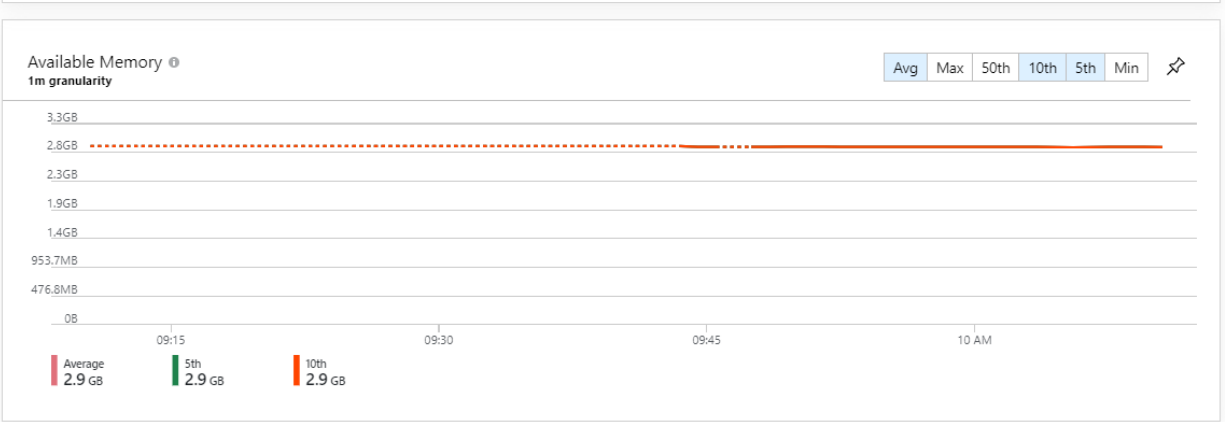
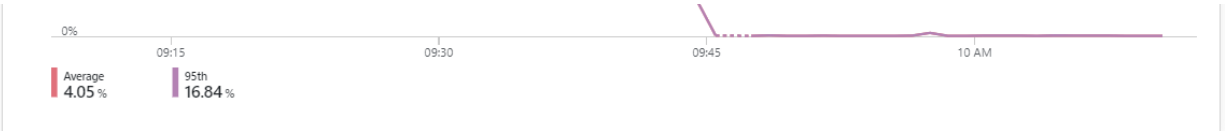
Time range: **Last hour as of 9 May 10:10**

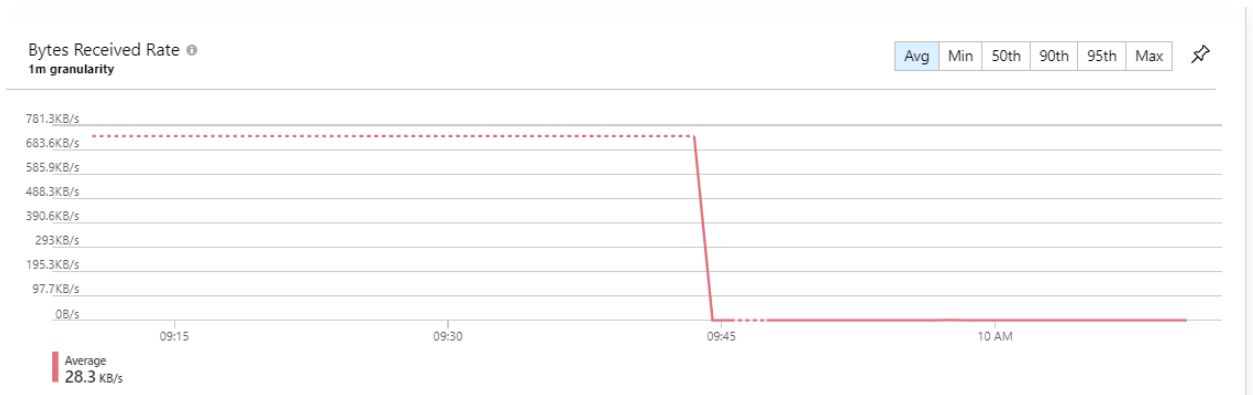
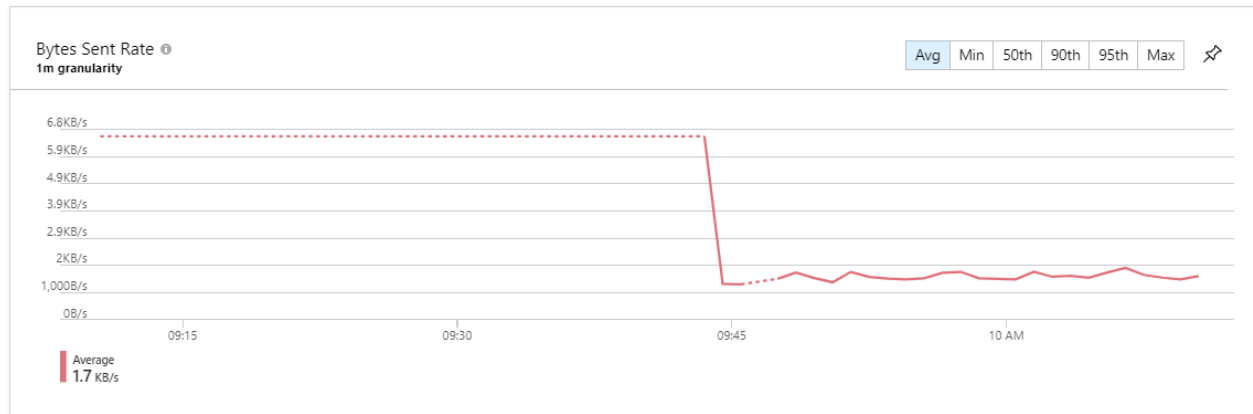
[View Workbooks](#) 

Logical Disk Performance

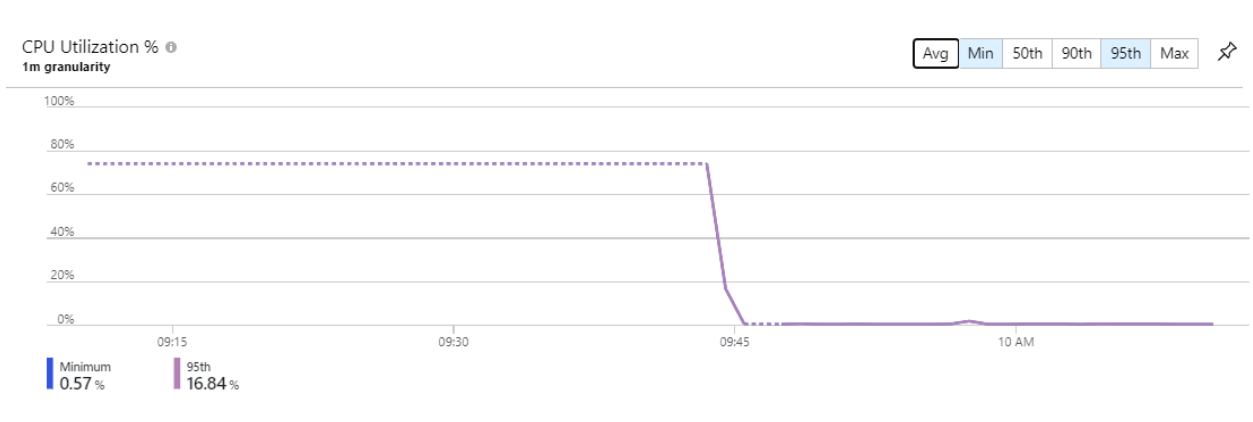
DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPs READ	P95 IOPs WRITE	P95 IOPs TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL
/	28.89	8%	33.21	4.88	55.8	0.72	0.52	2.23
/mnt	6.79	5%	0	0	0	0	0	0
Total	35.69	7%	33.21	4.88	55.8	0.72	0.52	2.23



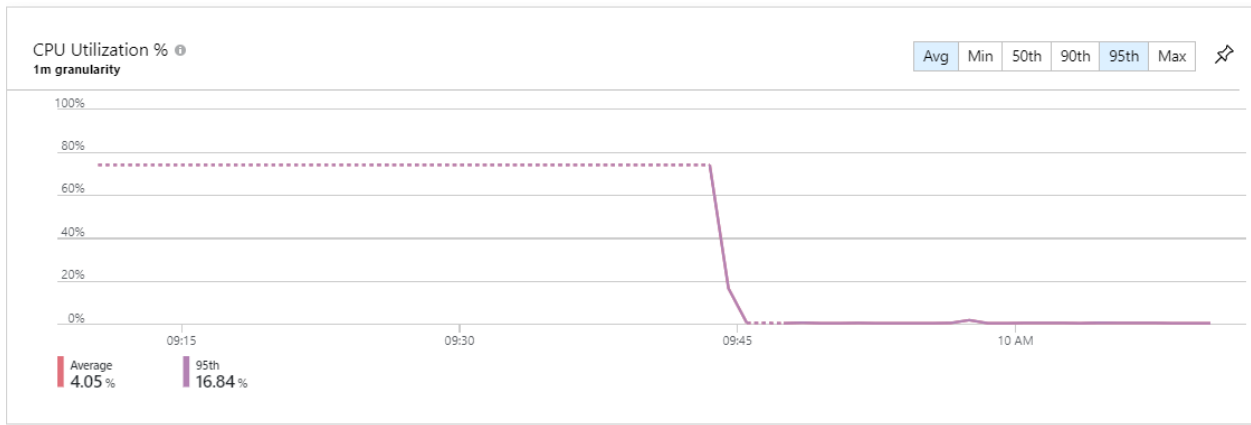




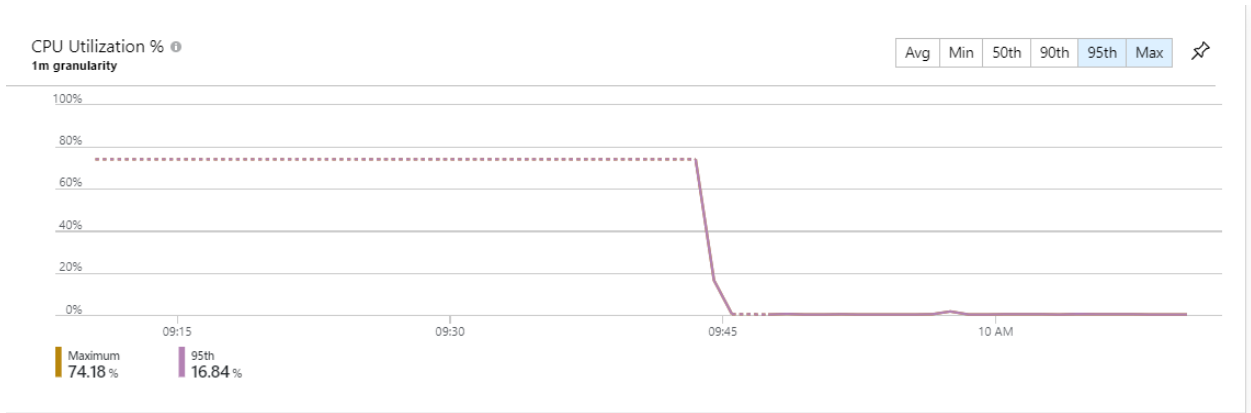
Data from Min CPU utilization



Data for Avg CPU utilization



Data for Max CPU utilization



Sample VM1 Insights

Home > SampleVM1

SampleVM1 | Insights

Virtual machine

Search

Resource Group Monitoring Azure Monitor Run Diagnostics Refresh Monitoring configuration Provide Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Availability + scaling

Configuration

Identity

Properties

Locks

Get started Performance Map

Time range: Last 30 minutes as of 9 May 10:07

3 Clients

SampleVM1 10 Processes

Port: 443 9 Servers

Port: 123 5 Servers

Port: 53 1 Servers

Port: 80 2 Servers

SampleVM1 Machine Summary

Properties Log Events Alerts Connections Changes

Quick links

Connection details

Fully Qualified Domain Name
SampleVM1

Operating System
Linux 5.4.0-1107-azure, Ubuntu 18.04.6 LTS

IPv4 Addresses
10.0.0.4/24


Health

Machine properties

Azure VM properties

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:

Home > SampleVM1 | Insights >

Logs ASH12345

New Query 1* x +

ASH12345 Select scope Time range: Last 30 minutes Save Share + New alert rule Export Pin to Format query

2 | where Computer == 'SampleVM1'

Tables Queries Functions ...

Search Filter Group by: Solution Collapse all

Favorites You can add favorites by clicking on the R icon

Azure Monitor for VMs AzureResources LogManagement Custom Logs

Results Chart

TimeGenerated [UTC]	Computer	Origin	Namespace	Name	Val	Tags	AgentId
> 5/9/2023, 7:43:48.021 AM	SampleVM1	vm.azm.ms/map	Computer	Heartbeat	1	("vm.azm.ms/processids":{"p-f1e1e2d5654c1483e3b52bda2...	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:44:47.925 AM	SampleVM1	vm.azm.ms/map	Computer	Heartbeat	1	("vm.azm.ms/processids":{"p-f1e1e2d5654c1483e3b52bda2...	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:45:48.085 AM	SampleVM1	vm.azm.ms/map	Computer	Heartbeat	1	("vm.azm.ms/processids":{"p-f1e1e2d5654c1483e3b52bda2...	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:46:47.989 AM	SampleVM1	vm.azm.ms/map	Computer	Heartbeat	1	("vm.azm.ms/processids":{"p-f1e1e2d5654c1483e3b52bda2...	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:47:05.000 AM	SampleVM1	vm.azm.ms	LogicalDisk	BytesPerSecond	0	("vm.azm.ms/mountid":"/mnt")	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:47:05.000 AM	SampleVM1	vm.azm.ms	LogicalDisk	ReadsPerSecond	0	("vm.azm.ms/mountid":"/mnt")	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:47:05.000 AM	SampleVM1	vm.azm.ms	LogicalDisk	WritesPerSecond	0	("vm.azm.ms/mountid":"/mnt")	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:47:05.000 AM	SampleVM1	vm.azm.ms	LogicalDisk	TransfersPerSecond	249970178557698	("vm.azm.ms/mountid":"/")	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:47:05.000 AM	SampleVM1	vm.azm.ms	LogicalDisk	TransfersPerSecond	0	("vm.azm.ms/mountid":"/mnt")	5cf5427e-99b1-4d9b-a912-387a0c55...
> 5/9/2023, 7:47:05.000 AM	SampleVM1	vm.azm.ms	LogicalDisk	ReadBytesPerSecond	0	("vm.azm.ms/mountid":"/mnt")	5cf5427e-99b1-4d9b-a912-387a0c55...

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

Virtual Machine 2 Insights:

SampleVM2 | Insights Virtual machine

Search

Resource Group Monitoring Azure Monitor Run Diagnostics Refresh Monitoring configuration Provide Feedback

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

Get started Performance Map

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%	0.02	3.38	3.38	0	0.02	0.02
/mnt	6.79	5%	0	0	0	0	0	0
Total	35.69	7%	0.02	3.38	3.38	0	0.02	0.02

CPU Utilization % 1m granularity

Avg Min 50th 90th 95th Max

0% 20% 40% 60% 80% 100%

09:30 09:45 10 AM 10:15

Average 0.76% 95th 1.77%

Available Memory 1m granularity

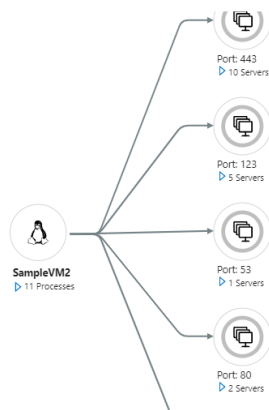
Avg Max 50th 10th 5th Min

0 953.7MB 1.4GB 1.9GB 2.3GB 2.8GB 3.3GB

09:30 09:45 10 AM 10:15

Average 2.9 GB 5th 2.9 GB 10th 2.9 GB

Time range: Last 30 minutes as of 9 May 10:21



View Workbooks

Legend

**SampleVM2**
Machine Summary[Properties](#) [Log Events](#) [Alerts](#) [Connections](#) [Changes](#)

Quick links

[Connection details](#)

Fully Qualified Domain Name

SampleVM2

Operating System

Linux 5.4.0-1107-azure, Ubuntu 18.04.6 LTS

IPv4 Addresses

10.0.0.5/24

> Health

> Machine properties

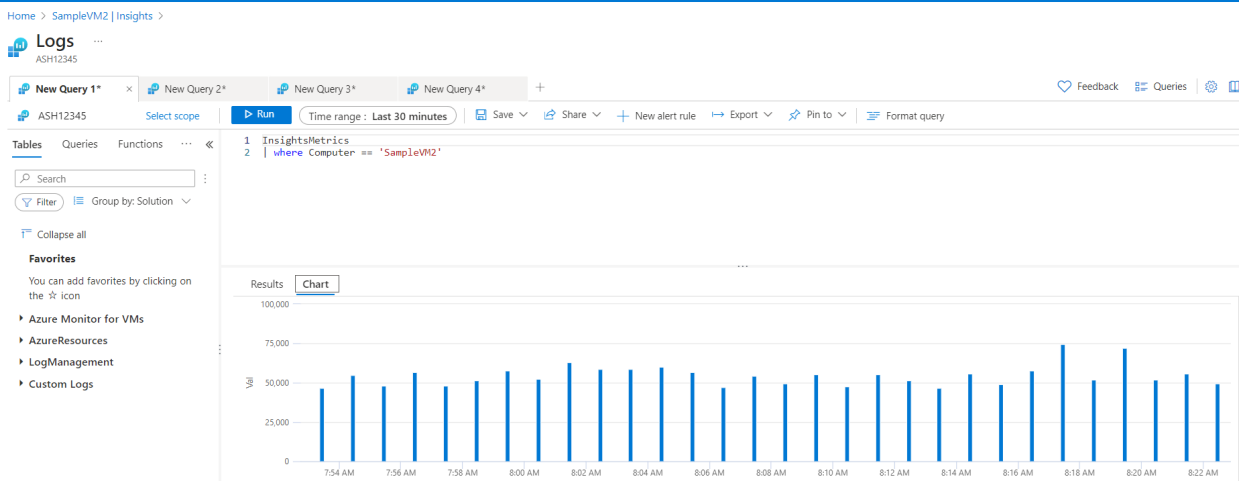
> Azure VM properties

**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

Home > SampleVM2 | Insights >

Logs ASH12345

New Query 1* x +

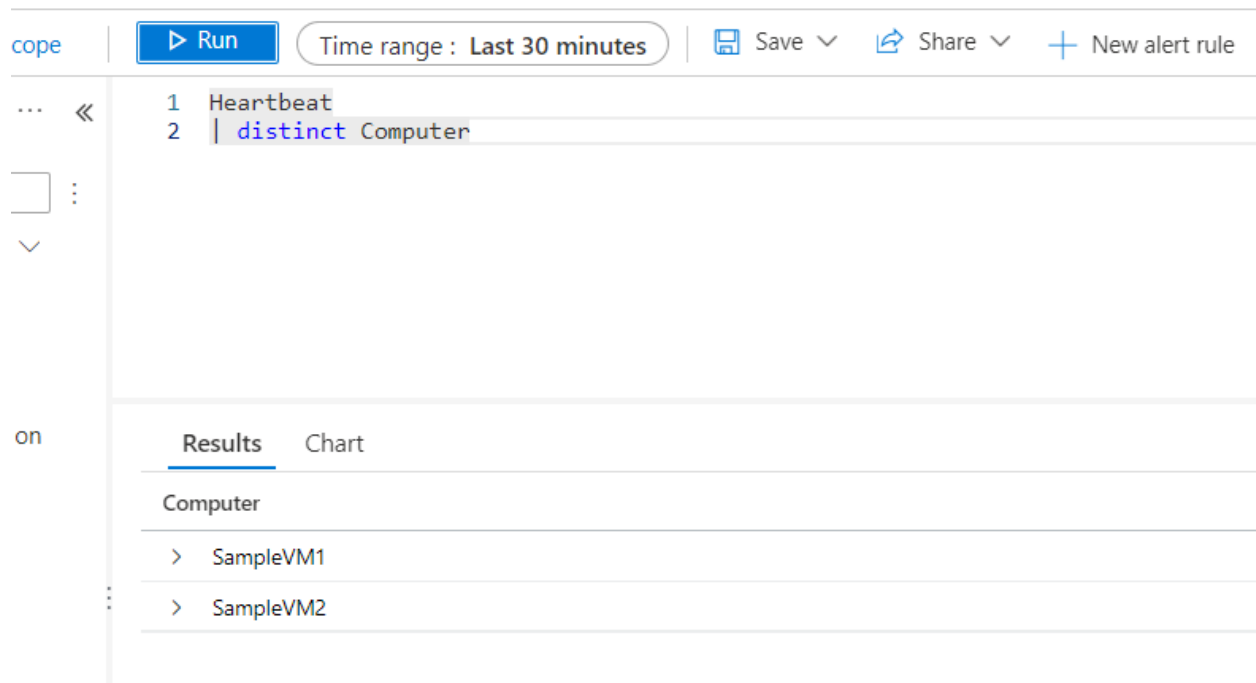
ASH12345 Select scope Run Time range: Last 30 minutes Save Share + New alert rule Export Pin to Format query

1 Heartbeat

Results Chart

TimeGenerated [UTC]	SourceComputerId	ComputerIP	Computer	Category	OSType	OSName
> 5/11/2023, 8:40:08.691 AM	af233b42-3694-4e6c-8dac-56d...	40.118.240.75	SampleVM2	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:40:27.108 AM	2b98c1fc-fe07-4c28-b391-1eb...	40.118.166.39	SampleVM1	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:41:08.691 AM	af233b42-3694-4e6c-8dac-56d...	40.118.240.75	SampleVM2	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:38:08.687 AM	af233b42-3694-4e6c-8dac-56d...	40.118.240.75	SampleVM2	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:42:07.795 AM	2b98c1fc-fe07-4c28-b391-1eb...	40.118.166.39	SampleVM1	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:42:25.766 AM	af233b42-3694-4e6c-8dac-56d...	40.118.240.75	SampleVM2	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:43:07.797 AM	2b98c1fc-fe07-4c28-b391-1eb...	40.118.166.39	SampleVM1	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:44:07.798 AM	2b98c1fc-fe07-4c28-b391-1eb...	40.118.166.39	SampleVM1	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:39:27.107 AM	2b98c1fc-fe07-4c28-b391-1eb...	40.118.166.39	SampleVM1	Direct Agent	Linux	Ubuntu
> 5/11/2023, 8:37:27.103 AM	2b98c1fc-fe07-4c28-b391-1eb...	40.118.166.39	SampleVM1	Direct Agent	Linux	Ubuntu

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)

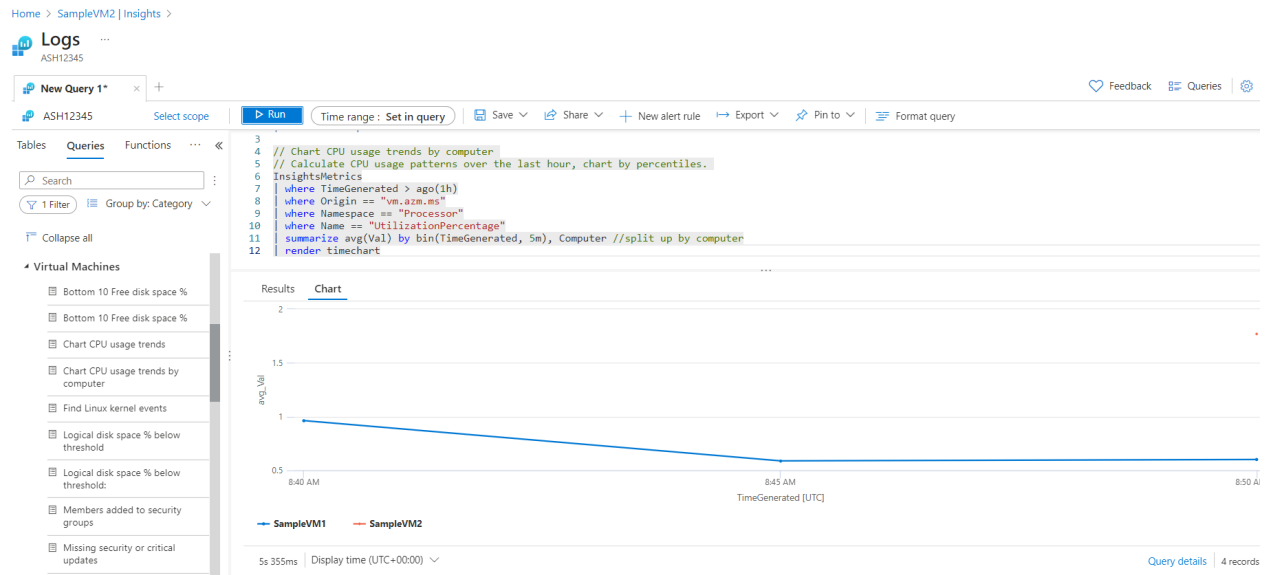
| where Origin == "vm.azm.ms"

| where Namespace == "Processor"

| where Name == "UtilizationPercentage"

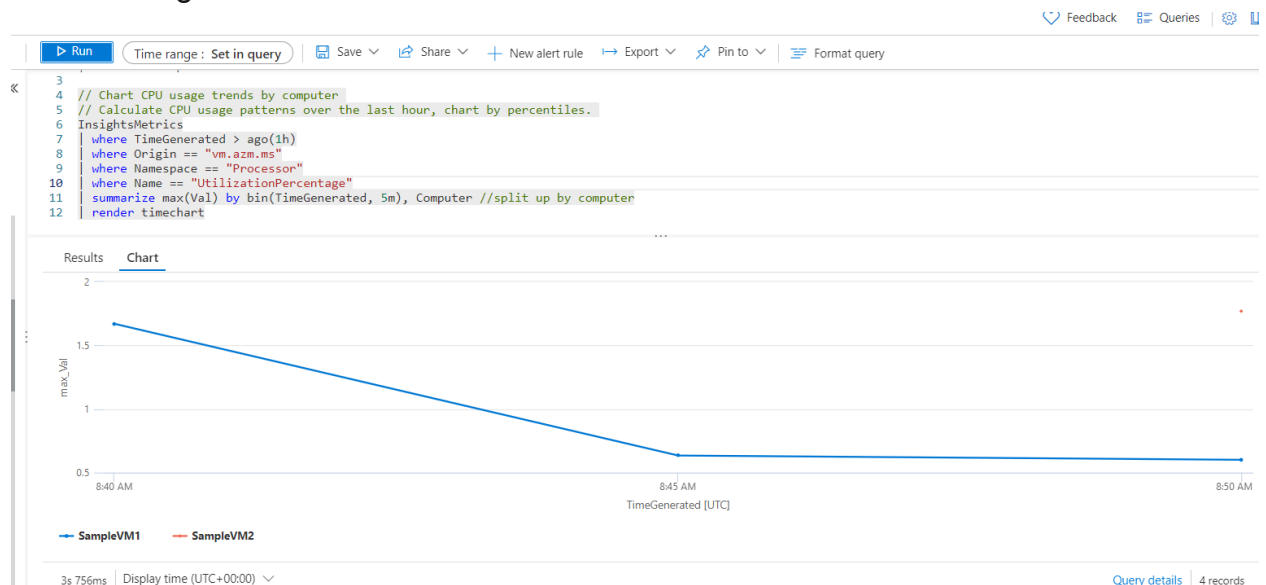
| summarize avg(Val) by bin(TimeGenerated, 5m), Computer //split up by computer

| 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

