Monitor performance of virtual machines by using Azure Monitor VM Insights

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

In this unit, you'll:

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.

## Create and configure a Log Analytics workspace

In the Azure portal we search for the Log Analytics Workplace and we click on Create. There we enter the following values:

|  |  |
| --- | --- |
| Property | Value |
| Subscription | Concierge Subscription |
| Resource group | [sandbox resource group name] |
| Name | xxxx-log-analytics |
| Region | Select the region closest to you. |

Create Log Analytics workspace 
Basics Tags Review + Create 
O 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 mrkspace. 
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 * G) 
Resource group* O 
Instance details 
Name* G) 
Region * (D 
Review + Create 
u Previous 
Concierge Subscription 
Create new 
west US 
Next : Tags 

After we enter the values, we go on **Review + Create > Create.**

Create Log Analytics workspace 
Validation passed 
Tags Review + Create 
Basics 
Log Analytics workspace 
by Microsoft 
Basics 
Subscription 
Resource group 
Name 
Region 
pricing 
Pricing tier 
Concierge Subscription 
learn -7 c3 fcc59-6dl c-4c58-89f8-d8a4bcd9ca6f 
xxxx- log-analytics 
West US 
Pay-as-you-go (Per 2018) 
The cost of your workspace depends on the volume of data ingested and how bng it is retained. Regional pricing details 
are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created. 
Learn more about Log Analytics pricing models. 
Tags 
None 
Create 
previous 
Download a template for automation 

When the resource deploys, we select **Go to resource.**

Microsoft.LogAnalyticsOMS I Overview 
Deployment 
Search 
Overview 
Inputs 
Outputs 
Template 
Delete Cancel t] Redeploy Download 
Your deployment is complete 
Deployment name: Microsoft.LogAnalyticsOMS 
Subscription: Concierge Subscription 
CD Refresh 
start time: 5/7/2023, 11:23:41 AM 
Correlation ID: Ob697886-7498-44f3-ab4d-90e39e879b5c 
Resource group: learn-7c3fcc59-6d1c-4c58-89f8-d8a4bcd9ca6f 
v Deployment details 
Next steps 
Go to resource 
Give feedback 
Tell us about your experience with deployment 

After the deployment is done, we go to **Properties** in the left menu and we look for the access control mode , and there we select **Use resource or workspace permissions.** This setting changes the access mode to use the resource-context.

b2a91S30-5546 
Settings 
Properties 
Resource ID 
_4dbf_81 c9_481 a 1497e5b4 
[subscriptions/bb493d80-b 1 a 540d6- b25a-60fc2a5497cO/resourc 
Subscription Name 
Concierge Subscription 
Subscription Id 
bb493d80-b1a5-40d6-b25a-60fc2a5497co 
Resource group 
learn- 7c3fcc59-6d 1 c4c58-89f8-d8a4bcd9ca6f 
Location 
Pricing tier 
Pay-as-pu-go 
Access control mode 
Use resource or workspace permissions (click to change) 

## Set up your environment

Here we will set up Virtual machines. We run these commands in the Azure Cloud Shell:

* For creating of VM1

az vm create \

--resource-group [sandbox resource group name] \

--location westus \

--name SampleVM1 \

--image UbuntuLTS \

--admin-username azureuser \

--generate-ssh-keys \

--verbose

A picture containing text, screenshot, font

Description automatically generated

* For creating of VM2

az vm create \

--resource-group [sandbox resource group name] \

--location westus \

--name SampleVM2 \

--image UbuntuLTS \

--admin-username azureuser \

--generate-ssh-keys \

--verbose

A screenshot of a computer screen

Description automatically generated with medium confidence

## Onboard virtual machines to Azure Monitor VM Insights

After we create the virtual machines, we go to Virtual Machines and select SampleVM1. In the left menu we select **Insights** and then we click **Enable.**

SampleVM1 1 Insights 
Virtual machine 
Monitoring 
Insights 
Alerts 
Metrics 
Diagnostic settings 
Logs 
Connection monitor (classic) 
Workbooks 
Autom ation 
Tasks (preview) 
Export template 
Help 
Resource health 
Boot diagnostics 
performance diagnostics 
VM Inspector (Preview) 
Resource Group MO 
Get mc 
With an Azure vi 
monitori' 
You will be billed 
The map data s 
monitored. For 
Enable 

Next, we need to select **Log Analytics agent**. After that we select the **Log Analytics workspace** we created. And we click **Configure**.

SampleVM1 1 Insights 
Virtual machine 
Monitoring 
Insights 
Alerts 
Metrics 
Diagnostic settings 
Logs 
Connection monitor (classic) 
Workbooks 
Autom ation 
Tasks (preview) 
Export template 
Help 
Resource health 
Boot diagnostics 
performance diagnostics 
VM Inspector (Preview) 
Resource Group MO 
Get mc 
With an Azure vi 
monitori' 
You will be billed 
The map data s 
monitored. For 
Enable  Monitoring configuration 
Virtual machine Insights now supports data collection using the Azure Monitor agent. Configuring using the , 
in preview mode. 
Enable insights using 
Subscription 
Log Analytics workspaces 
C) Azure Monitor agent (Recommended) 
@ Log Analytics agent 
Concierge Subscription 
xxxx-log-analytics 

We do the same for SampleVM2.

SampleVM2 1 Insights 
Virtual machine 
P Search 
Monitoring 
Insights 
Alerts 
Metrics 
Diagnostic settings 
Logs 
Connection monitor (classic) 
Workbooks 
Tasks (preview) 
Export template 
Help 
Resource health 
Boot diagnostics 
Performance diagnostics 
VM Inspector (Preview) 
Reset password 
Virtual machine Insights now supports data collection using the Azure Monitor agent. Configuring using the 
in preview mode. 
Enable insights using 
Subscription * 
Log Analytics workspaces 
o 
Azure Monitor agent (Recommended) 
• Log Analytics agent 
Concierge Subscription 
xxxx-log-analytics 
Configure 
Cancel 

After 5 to 10 minutes, both VM’s should be configured. Then we go to Insights again and we review the map. The map displays dependencies like processes running, ports open, connection details, health of the virtual machine, machine properties, and Azure virtual machine properties.

SampleVMI I Insights 
Virtual machine 
Resource Group Monitoring Azure Monitor 
Run Diagnostics C.) Refresh Monitoring configuration Provide Feedback 
The virtual machine is currently using Log Analytics agent. Azure Monitor Agent is now available. 
Get started Performance Map 
O Legend 
A SampleVM1 
Machine Summary 
Properties Log Events Alerts 
Quick links 
Connection details 
Fully Qualified Domain Name 
SampleVM1 
Operating System 
Connections 
Changes 
Linux 5.40-1107-azure, Ubuntu 18.046 LTS 
I PWI Addresses 
10.0.0.4/24 
Health 
Machine properties 
Azure VM properties 

SampleVM2 1 Insights 
Virtual machine 
Resource Group Monitoring Azure Monitor 
Run Diagnostics C_) Refresh Monitoring configuration 
The virtual machine is currentlyusing Log Analytics agent Azure Monitor Agent is now available. 
C) Provide Feedback 
Get started Performance Map 
Time range: Last 30 minutes as Of 7 May 11:48 
View Workbooks 
O Legend 
SampleVM2 
Machine Summary 
Properties Log Events 
Quick links 
Connection details 
Alerts 
Connections 
Changes 
Fully Qualified Domain Name 
SampleVM2 
Operating System 
Linux 5.40-1107-azure, Ubuntu 18.046 L TS 
IPv4 Addresses 
10.005/24 
Health 
Machine properties 
Azure VM properties 

We select the Performance tab for both VM’s.

SampleVMI I Insights 
Virtual machine 
Resource Group Monitoring Azure Monitor 
Run Diagnostics CD Refresh Monitoring configuration 
The virtual machine is currently using Log Analytics agent. Azure Monitor Agent is now available. * 
Get started Performance Map 
Time range: Last hour as of 7 May 11:49 
Logical Disk Performance 
CURRENTSIZE(GB) P9S10PsREAD P9S10PsWRITE 
CPU Utilization % o 
1m vanuIariW 
11 AM 
provide Feedback 
P" MB/' WRITE MB's TOTAL 
View Workbooks 
P95 lops TOTAL 
MB's READ 
1:30 
Avg 
Min 
50th 90th 
95th 
Max 

SampleVM2 1 Insights 
Virtual machine 
Resource Group Monitoring Azure Monitor 
Run Diagnostics C_) Refresh Monitoring configuration 
The virtual machine is currently using Log Analytics agent. Azure Monitor Agent is now available. -9 
Get started Performance Map 
Time range: Last hour as Of 7 May 11:50 
Logical Disk Performance 
CURRENTSIZE(GB) P9SIOPsREAD P9SIOPsWRITE P9SIOPsTOTAL 
Provide Feedback 
View Workbooks 
pgs MB,'sWRITE pgs MB," TOTAL 
CPU Utilization % 0 
pgs MB," READ 
11:30 
95th 
1 IAS 
Max 
11 AM 
No Data 
11:15 
Avg 
Min 
50th 
90th 

There are 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

Next, we select **Log Events,** and then we select **InsightMetrics** row from the table.

SampleVMI 
Machine Log Events 
Properties Log Events Alerts Changes 
Select an event type to open in Log AnaSrtics 
Heartbeat 
InsightsMetrics 
ServiceMapComputer_CL 
Service Map Process_CL 
VMBoundPort 
VMComputer 
VMConnection 
VMProcess 
13 
17 
63 
17  SampleVM2 
Machine Log Events 
Properties Log Events Alerts Changes 
Select an event type to open in Log Analytics 
Heartbeat 
InsightsMetrics 
ServiceMapComputer_CL 
ServiceMapProcess_CL 
VMBoundPort 
VMComputer 
VMConnection 
VMProcess 
47 
2 
72 

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

Logs 
AA-log-analytics 
New Query I • 
xxxx-log-analytics 
x 
Select scope 
> Run 
Time range : 
Last hour 
• SampleVM1 • 
Computer 
SampleVM1 
SampleVM1 
SampleVM1 
SampleVM1 
SampleVM1 
SampleVM1 
SampleVMl 
SampleVMl 
Save v 
vmazm.ms/map 
vmazm.ms/map 
vm.azm.ms/map 
vm.azm.ms/map 
vm.azm.ms/map 
vm.azm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
Share v 
+ New alert rule 
Export v 
pinto v 
Feedback 
Format query 
Queries 
Tables Queries Functions 
P Search 
Y Filter Group by: Solution 
Collapse all 
Favorites 
You can add favorites by clicking on 
the icon 
Azure Monitor for VMS 
AzureResources 
LogManagement 
Custom Logs 
1 
2 
InsightsMetrics 
I L•mere Computer — 
Results Chart 
TimeGenerated [UTC) 
5/7/2023, AM 
5/7/2023, 94011.913 AM 
5/7/2023, AM 
5/7/2023, AM 
5/7/2023, 9:4311881 AM 
5/7/2023, AM 
5/7/2023, AM 
5/7/2023, AM 
Namespace 
Computer 
Computer 
Computer 
Computer 
Computer 
Computer 
Computer 
Computer 
Name 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Val 
Tags 
Cvm.azm.ms/processlds 
Cvm.azm.ms/processlds 
Cvm.azm.ms/processlds 
Cvm.azm.ms/processlds 
Cvm.azm.ms/processlds 
Cvm.azm.ms/processlds 
Cvm.azm.ms/processlds 
.azm. m ds 
Agent Id 
dbfd41 e 7 
-bd45-4 
dbfd41e7-bd4S-4 
dbfd41e7-bd4S-4 
dbfd41e7-bd4S-4 
dbfd41e7-bd4S4 
dbfd41e7-bd4S4 
dbfd41e7-bd454 
dbfd41e7-bd4S4 

Logs 
xxxx-log-analytics 
New Query I 
xxxx-log-analytics 
x 
New Query 
Select scope 
> Run 
Time range : 
1 
Last hour 
where Computer = 
Computer 
SampleVM2 
SampleVM2 
sampleVM2 
sampleVM2 
sampleVM2 
sampleVM2 
sampleVM2 
sampleVM2 
Save v Sh a re v 
+ New alert rule 
Export v 
pinto v 
Feedback 
Format query 
Tables Queries Functions 
P Search 
Y Filter Group by: Solution 
Collapse all 
Favorites 
You can add favorites by clicking on 
the icon 
Azure Monitor for VMS 
AzureResources 
LogManagement 
Custom Logs 
Insightsmetrics I 
Results Chan 
TimeGenerated (LJTCI 
5/7/2023, AM 
5/7/2023, AM 
5/7/2023, 94526950 AM 
5/7/2023, AM 
5/7/2023, 94726758 AM 
5/7/2023, AM 
5/7/2023, 94826918 AM 
5/7/2023, 94326886 AM 
• SampleVM2 ' 
Origin 
vmazm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
vmazm.ms/map 
Namespace 
Computer 
Computer 
Computer 
Computer 
Computer 
Computer 
Computer 
Computer 
Name 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Heartbeat 
Val 
Tags 
Cvm.azm.ms/processlds 
rvm.azm.ms/processlds 
rvm.azm.ms/processlds 
rvm.azm.ms/processlds 
rvm.azm.ms/processlds 
rvm.azm.ms/processlds 
rvm.azm.ms/processlds 
rvm.azm.ms/processlds 
Queries 
Agent Id 
3eb838b3- 
3eb838b3-6953-4 
3eb838b3-6953-4 
3eb838b3-6953-4 
3eb838b3-6953-4 
3eb838b3-6953-4 
3eb838b3-69534 
3eb838b3-69534 
2s457ms Display time (UTC.OO:OO) 
Query details 
1-90f71 

# Exercise - Build log queries

In this unit, you'll:

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

## Build a query by using the query pane

In the Azure portal, we search for Log Analytics Workspace and select the workspace we created earlier.

Log Analytics workspaces 
Microsoft Learn Sandbox 
+ Create Open recycle bin Manage view v 
Filter for any field.„ 
Showing I to I Of I records. 
Name t 
kxxx-log-analytics 
Subscription equals all 

Under **General** we select **Logs** and the **Queries** page will open.

xxxx-log-analytics I Logs 
Log Analytics workspace 
Search 
Overview 
Activity log 
Access control (IAM) 
Tags 
Diagnose and solve problems 
Logs 
Settings 
Tables 
Agents 
Usage and estimated costs 
Data export 
Network isolation 
Linked storage accounts 
Properties 
Locks 
Classic 
Legacy agents management 
Always show Queries @ 
x 
x 
Queries 
Query packs: Select query packs 
Catego ry 
Favorites 
All Queries 
Applications 
Audit 
Azure Monitor 
Azure Resources 
Azure Virtual Deskt... 
Containers 
Databases 
Desktop Analytics 
IT & Management 
Network 
P Search 
CCF application errors 
View the latest Confidential Consortium 
Framework application errors. 
Run 
Response time trend 
Chart request duration over the last 12 hours. 
Run 

We can group them by **Category**.

xxxx-log-analytics I Logs 
Log Analytics workspace 
New Query I 
xxxx-log-analytics 
Select scope 
Tables Queries Functions 
p Search 
Group by: Category v 
Collapse all 
You can add favorites by clicking on 
the icon 
Applications 
Run 
1 Type y 
Queries I 

Or we can group them by **Resource type.** There we can select **Virtual Machine Scale Sets.** Under that we select **Chart CPU usage trends by computer** query, and we select **Run**.

D xxxx-log-analytics I Logs 
Log Analytics workspace 
New Query I 
xxxx-log-analytics Select scope 
Tables Queries Functions Filter 
p virtual machine 
Group by: Resource type v 
Y Filter 
Collapse all 
Favorites 
You can add favorites by clicking on 
the icon 
• Virtual Machine Scale Sets 
> Run 
1 
Time range: Last 24 hours 
Type your query here or click one of the queries to start 
E 
E 
Bottom 10 Free disk space % 
Chart CPU usage trends by computer 
Logical disk space % below threshold 
Top 10 Virtual Machines by CPU utilization 
Track VM Availability using Heartbeat 
Virtual Machine available memory 
Virtual Machine free disk space 
What data is being collected? 
Chart CPU usage trends by computer 
Run Load to editor 
Description 
Calculate CPU usage patterns over the last hour, chart by percentiles. 
Information 
Example query - Created by Microsoft 
Resource type: Virtual Machine Scale Sets Category. Virtual Machines 
Topic: Performance Query type: Example q ueries 

This query:

1. Takes data from the InsightsMetrics table.
2. Looks at all data values ingested over the last hour underneath the Processor namespace.
3. Returns the rounded average value in 5-minute intervals for both machines.

Run 
Time range: Set in query Save Share -4— New alert rule Export v 
// Chart CPU usage trends by computer 
// Calculate CPU usage patterns over the last hour, chart by percentiles. 
InsightsMetrics 
I where TimeGenerated > ago(lh) 
I where Origin - 
"vm. azm. ms" 
I where Namespace - 
"Processor 
I where Name - 
"Utilization percentage" 
I sumarize avg(Va1) by bin(TimeGenerated, 5m), Computer //split up by computer 
I render timechart 
Pinto 
1 
2 
3 
4 
5 
6 
7 
8 
9 
Resu Its 
Chart 
1035 AM 
SampleVM 1 
AM 
10.45 AM 
T.meGenerated [UTC) 
— SampleVM2 
4s 135ms Display time (UTC •00:00) 
Format query• 
10:50 AM 
Query details 
loss AM 
8 records 

We can edit the existing query. Instead of summarize avg(Val) we will change it to summarize max(Val). We run the query and analyze the results.

This edited query:

1. Takes data from the InsightsMetrics table.
2. Looks at all data values ingested over the last hour underneath the Processor namespace.
3. Returns the rounded maximum value in 5-minute intervals for both machines.

a. Queries 
Run 
Feedback 
Format query 
save v é 
Time range: Set in query 
// chart CPU usage trends by computer 
// calculate CPU usage patterns over the 
Insightsmetrics 
I where TimeGenerated > ago(lh) 
I where origin " 
vm. azm.ms " 
I where Namespace • 
• processor" 
izationpercentage" 
+ New alert rule Export v 
Share v 
last hour, chart by percentiles. 
4 
6 
7 
8 
9 
I sumrnarize max Val by bin(TimeGenerated, 
I ren er Imec a 
5m), computer //split up by 
Results 
Chart 
10-45 AM 
AM 
10±5 AM 
11:00 AM 
S? Pinto v 
11:05 AM 
1040 AM 
SampleVM2 
11:10 AM 
TimeGenerated IUTCI 
SampleVMl 
2s 180ms Display time (UTC +00:00) v 
11:15 AM 
Query details 
11:20 AM 
18 records 

We can pin each of these visualizations to a dashboard by selecting Pin to dashboard at the top and specify the following:

* Create a new dashboard or add to an existing dashboard.
* If existing, deploy the new visualization to the appropriate shared or private dashboard.
* If new, determine if the dashboard will be a private or shared dashboard.
* If new, name the dashboard.
* If new, specify where the dashboard will be deployed.