Implement Monitoring

(LAB-204-11-01)

Lab scenario

You need to evaluate Azure functionality that would provide insight into performance and configuration of Azure resources, focusing in particular on Azure virtual machines. To accomplish this, you intend to examine the capabilities of Azure Monitor, including Log Analytics.

Objectives

In this lab, you will:

- Provision the environment
- Create and configure an Azure Log Analytics workspace
- Review default monitoring settings of Azure virtual machines
- Configure Azure virtual machine diagnostic settings
- Review Azure Monitor functionality
- Review Azure Log Analytics functionality
- Review Azure Activity Log functionality

Task 1: Provision Azure Resources

In this task, you will deploy a virtual machine that will be used to test monitoring scenarios.

Step 1: Create Virtual Machine

1. Click the **virtual machines** link in the left-hand navigation bar.

2. Click the **Create** button to start the creation process.

3. You will be required to **fill in specific information** regarding your virtual machine, including:

    a. **Subscription**: Select **Default subscription**

    b. **Resource Group**: Create **new** resource group **Az-204-11-01-RG**

    c. **Virtual Machine Name**: Write **LAB-204-11-VM**

d. **Region**: Select region **West US2**

e. **Image**: Dropdown and Select **Windows Server 2019 Datacenter**

f. **Size**:

  i. Select **Change size**

  ii. Search & **Select** **B2ms** virtual machine

g. **Administrator Account**:

  i. **Username**: Write **master**

  ii. **Password**: Write **Lab@password**

h. **Inbound Port Rules**:

  i. **Public inbound ports**: Select **Allow selected ports**

  ii. **Select inbound ports**:

    a. Dropdown and select **RDP (3389)**

    b. Dropdown and select **HTTP (80)**

Note: Leave other details as default.

4. Click the **Next: Disks** to continue

Note: Leave all the details as default.

5. Click the **Next: Networking** to continue.

Note: Leave all the details as default.

6. Click the **Next: Management** to continue.

  i. **Boot diagnostics**: Select **Disable**.

  ii. **Enable auto-shutdown**: **Uncheck** the Option.

Note: Leave the other details as default.

7. Click on the **Next: Advanced** to continue

Note: Leave the other details as default.

8. Click the **Next: Tags** to continue.

Note: Leave the other details as default.

9. Click the **Next: Review + create** button to continue.

Note: **Wait**, unless you see the **validation passed** message. If not verify each step of configuration from starting.

Task 2: Create Azure Log Analytics Workspace

In this task, you will create and configure an Azure Log Analytics workspace.

Step 1: Register Microsoft Services

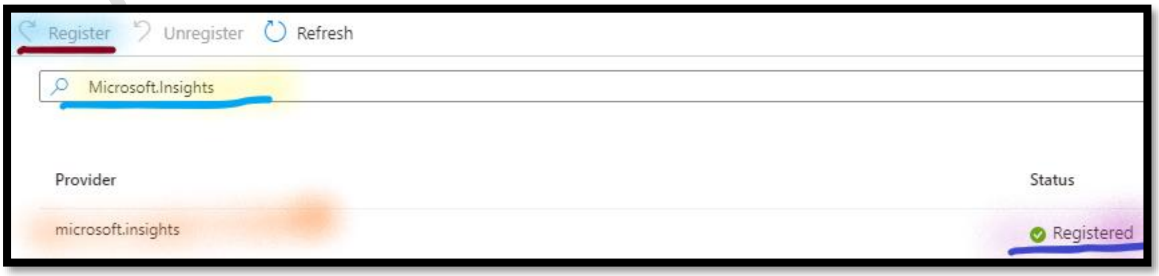
10. From the Azure Portal, go to the left menu, Select **All Services**.
11. Search and Select **Subscriptions** under **All Services**.
12. Select your **Default subscriptions**

Register Microsoft.Insight

a. Under settings, select **Resource Providers**.

b. Search **Microsoft.Insights**.

c. **Register** the **Microsoft.Insight**, if status is showing as **NotRegister**.



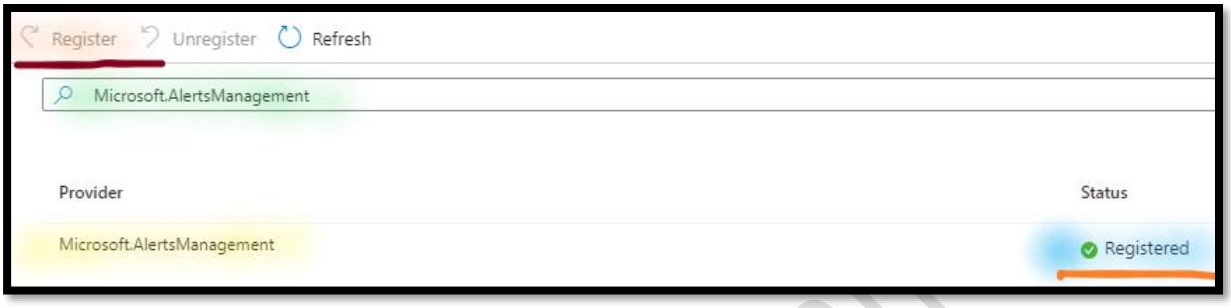
Provider	Status
microsoft.insights	Registered

13.Under settings, select **Resource Providers**.

Register Microsoft.AlertsManagement

a. Search **Microsoft.AlertsManagement**.

b. **Register** the **Microsoft.AlertsManagement**, if status is showing as **NotRegister**.



Microsoft.AlertsManagement

Provider	Status
Microsoft.AlertsManagement	Registered

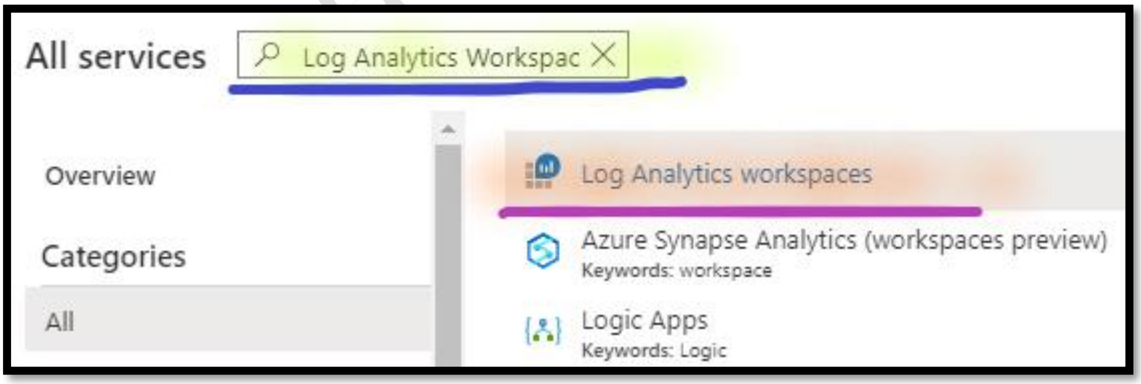
Note: **Wait**, till status showing **Registered**, for Insights and AlertsManagement. It takes **~10-15 mnts**.

Step 2: Create Azure Log Analytics Workspace

14.From the Azure Portal, go to the left menu, Select **All Services**.

15.Search and Select **Log Analytics workspaces** under all services

16. Select **Create** and **configure**:



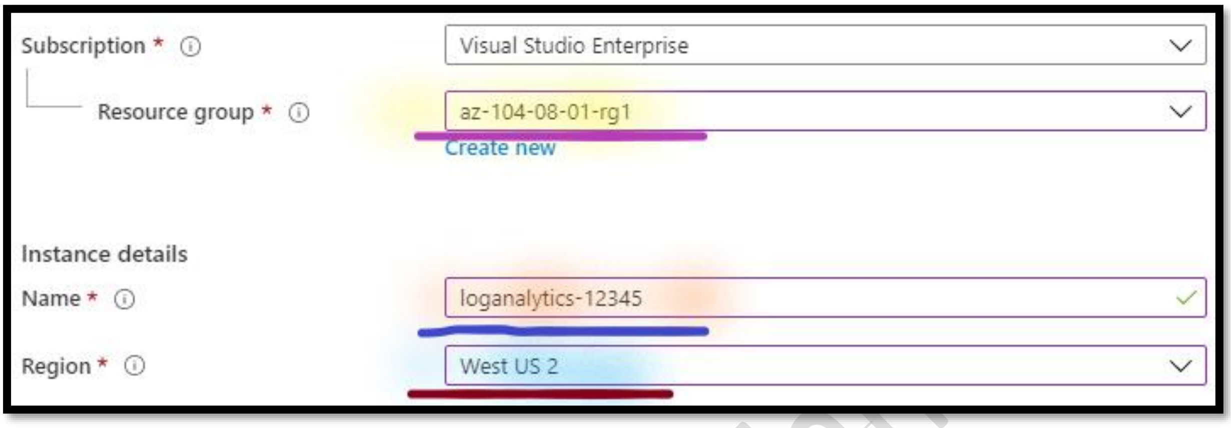
a. **Subscription**: Select your **Default subscription**

b. **Resource Group**: Dropdown & Select **AZ-204-11-01-RG**

c. **Name**: Write **loganalytics-123**

Note: Replace **123** to make the name unique.

d. **Region**: Dropdown and Select **West US2**



Subscription * Visual Studio Enterprise

Resource group * az-104-08-01-rg1

Instance details

Name * loganalytics-12345

Region * West US 2

e. Select **Next: Pricing Tier**

Note: Leave other details as default.

f. Select **Next: Tags**

Note: Leave other details as default.

g. Select **Next: Review + Create**

h. Select **Create**

Note: **Wait**, till deployment gets **completed**.

Step 2: Configure Log Analytics

17. From Azure portal, go to left side, select **Virtual machines**

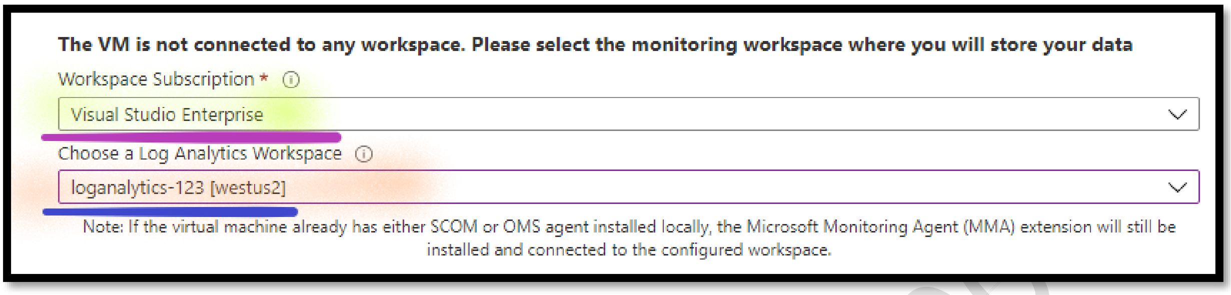
18. Select & Open **Az204-11-VM** virtual machine

19. Select **Logs** under **monitoring**

    a. Select **Enable**.

i. Workspace Subscription: Dropdown and Select your **Default Subscription**.

ii. **Log analytics workspace**: Dropdown and Select **loganalytics-123**



The VM is not connected to any workspace. Please select the monitoring workspace where you will store your data

Workspace Subscription * ⓘ: Visual Studio Enterprise

Choose a Log Analytics Workspace ⓘ: loganalytics-123 [westus2]

Note: If the virtual machine already has either SCOM or OMS agent installed locally, the Microsoft Monitoring Agent (MMA) extension will still be installed and connected to the configured workspace.

iii. Select **Enable**.

Note: **Don't Wait**, go to the next step.

Task 3: Review the Metrics

In this task, you will review default monitoring settings of Azure virtual machines.

Step 1: Review the CPU metrics using Metrics Explorer

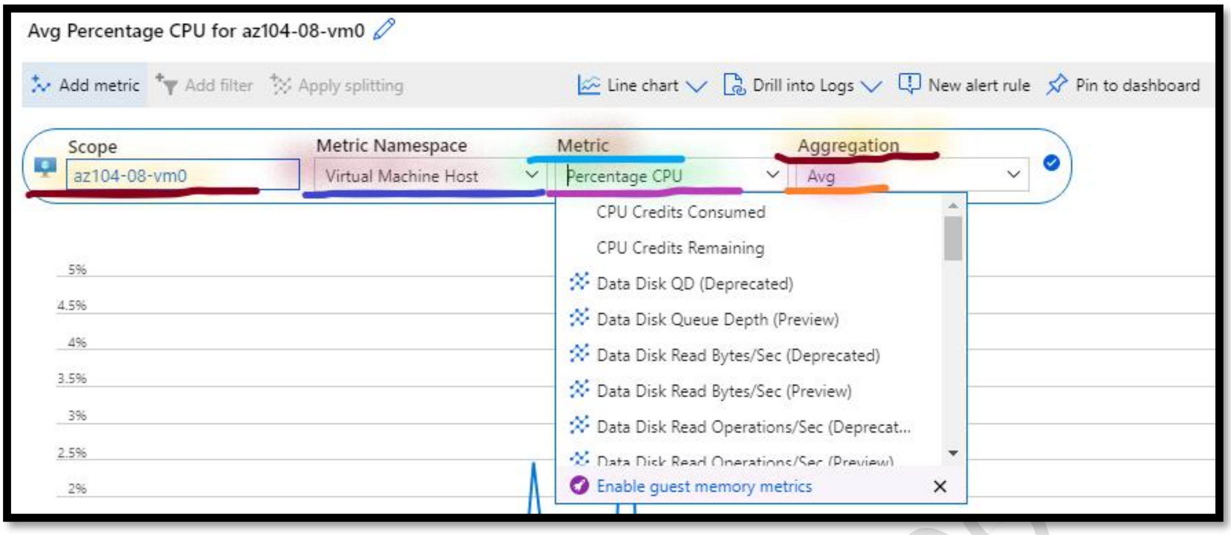
20. From Azure portal, go to left side, select **Virtual machines**

21. Select & Open **Az204-11-VM** virtual machine

22. Select **Metrics** under **monitoring**

   b. In the **Metric drop-down list**, review the list of available metrics.

Note: The list includes a range of CPU, disk, and network-related metrics that can be collected from the virtual machine host, without having access into guest-level metrics.



Avg Percentage CPU for az104-08-vm0

Scope: az104-08-vm0

Metric Namespace: Virtual Machine Host

Metric: Percentage CPU

Aggregation: Avg

Add metric
Add filter
Apply splitting
Line chart
Drill into Logs
New alert rule
Pin to dashboard
CPU Credits Consumed
CPU Credits Remaining
Data Disk QD (Deprecated)
Data Disk Queue Depth (Preview)
Data Disk Read Bytes/Sec (Deprecated)
Data Disk Read Bytes/Sec (Preview)
Data Disk Read Operations/Sec (Deprecat...
Data Disk Read Operations/Sec (Preview)
Enable guest memory metrics
5%
4.5%
4%
3.5%
3%
2.5%
2%

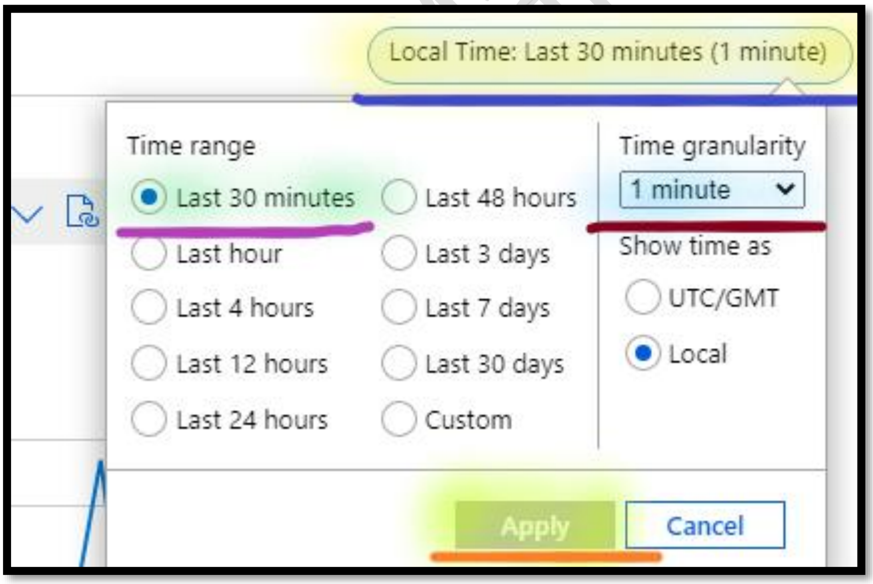
i. **Metric**: Dropdown and Select **Percentage CPU**.

ii. **Aggregation**: Dropdown and Select **Avg**.

c. **Go to the right** site, Click on **Local time**.

i. **Time range**: Select **Last 30 minutes**.

ii. **Time granularity**: Dropdown and Select **1 minute**.



Local Time: Last 30 minutes (1 minute)

Time range

● Last 30 minutes ○ Last 48 hours

○ Last hour ○ Last 3 days

○ Last 4 hours ○ Last 7 days

○ Last 12 hours ○ Last 30 days

○ Last 24 hours ○ Custom

Time granularity: 1 minute

Show time as

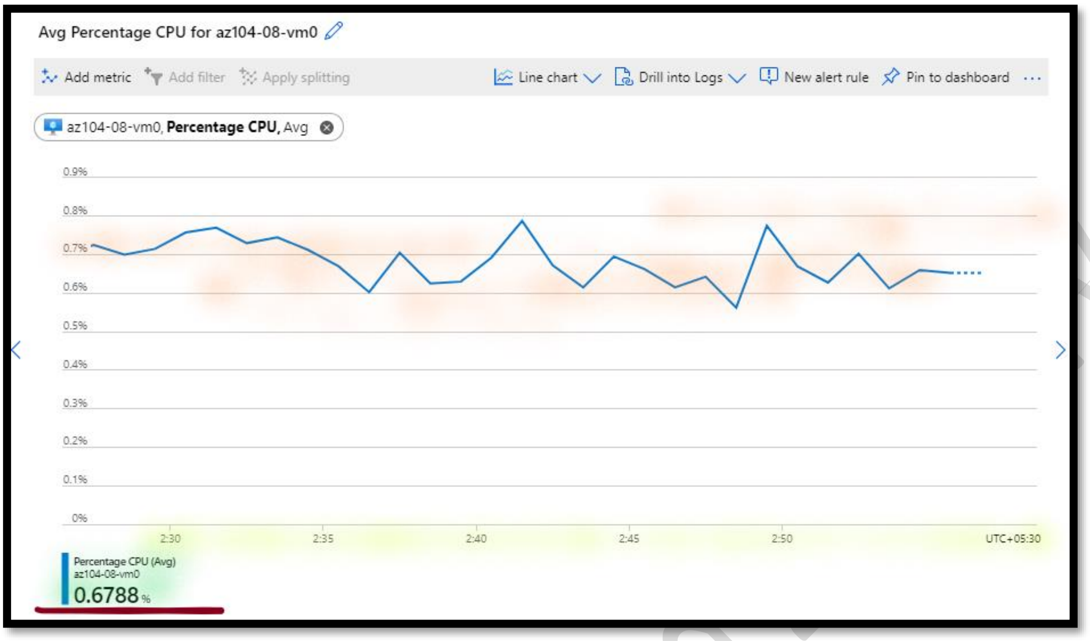
○ UTC/GMT

● Local

iii. Select **Apply**.

Note: **Review**, the resulting results.

Note: If you get **Error retrieveing data**, **Wait**, for mnts. and Refresh your Screen to view the metrics.



Note: You can also **add additional metrics** to view from theh same dashboard.

Task 4: Configure Azure VM Diagnostic Settings

In this task, you will configure Azure virtual machine diagnostic settings.

Step 1: Enable Guest Level Monitoring

23. From Azure portal, go to left side, select **Virtual machines**

24. Select & Open **Az204-11-VM** virtual machine

25. Select **Diagnostic settings** under **monitoring**

    a. **Diagnostic storage account**: Select **Create new**

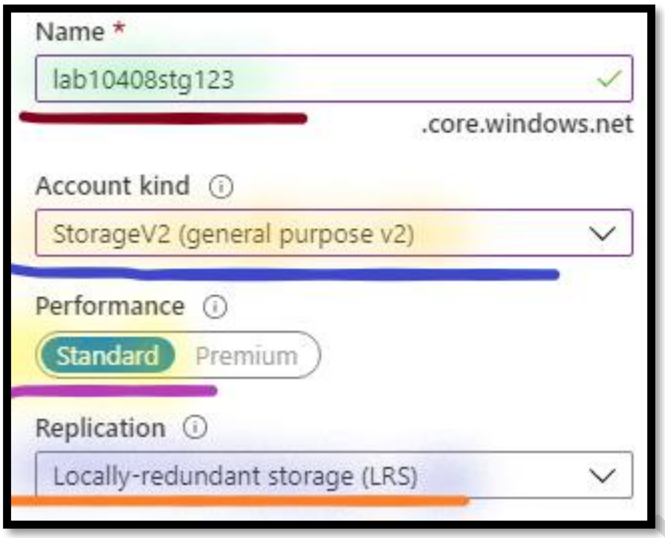
       i. **Name**: Write **lab20408stg123**

Note: **Replace 123**, to make the storage account name unique.

       ii. **Account kind**: Dropdown and Select **Storage v2**

iii. **Performance**: Select **Standard**

iv. **Replication**: Dropdown and Select **Locally-redundant storage (LRS)**



Name *

lab10408stg123 ✓

.core.windows.net

Account kind ⓘ

StorageV2 (general purpose v2)

Performance ⓘ

● Standard ○ Premium

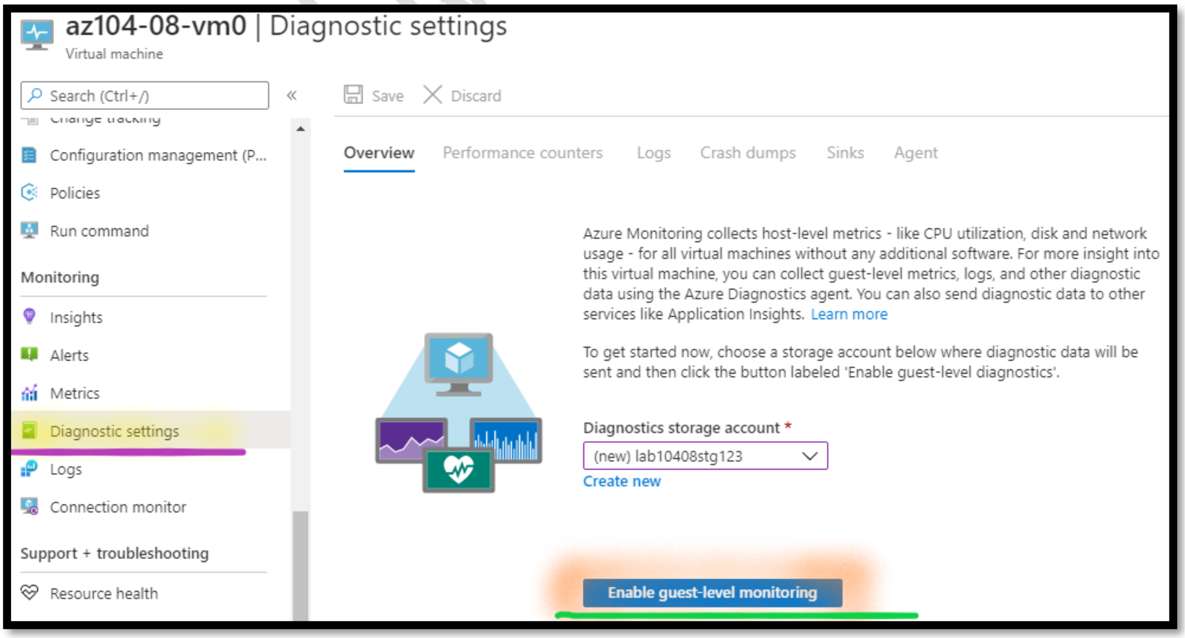
Replication ⓘ

Locally-redundant storage (LRS)

v. Select **Ok**

b. Select **Enable guest-level monitoring**

Note: **Wait**, till **diagnostic settings** gets enabled. It takes **~5 mnts**.



az104-08-vm0 | Diagnostic settings

Virtual machine

Azure Monitoring collects host-level metrics - like CPU utilization, disk and network usage - for all virtual machines without any additional software. For more insight into this virtual machine, you can collect guest-level metrics, logs, and other diagnostic data using the Azure Diagnostics agent. You can also send diagnostic data to other services like Application Insights. Learn more

To get started now, choose a storage account below where diagnostic data will be sent and then click the button labeled 'Enable guest-level diagnostics'.

Diagnostics storage account *

(new) lab10408stg123

Create new

Enable guest-level monitoring

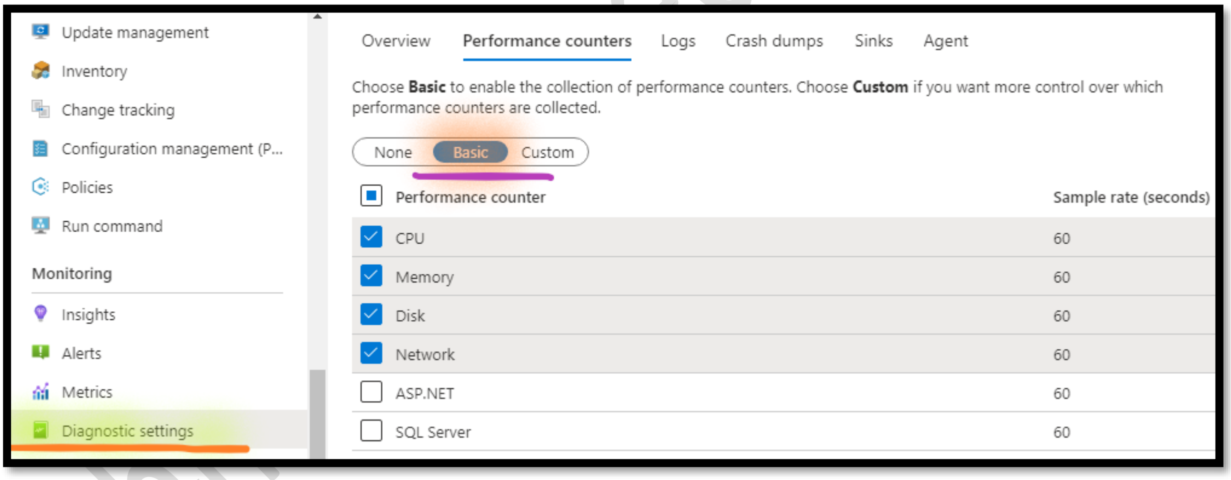
Note: **Wait**, till deployment gets completed.

Step 2: View the Performance Counters

26. From Azure portal, go to left side, select **Virtual machines**
27. Select & Open **Az204-11-VM** virtual machine
28. Select **Diagnostic settings** under **monitoring**
29. Select **Performance counters**

Note: **Review**, the available counters.

Note: By default, CPU, memory, disk, and network counters are enabled. You can switch to the Custom view for more detailed listing.



Choose **Basic** to enable the collection of performance counters. Choose **Custom** if you want more control over which performance counters are collected.

None [✓ Basic] Custom

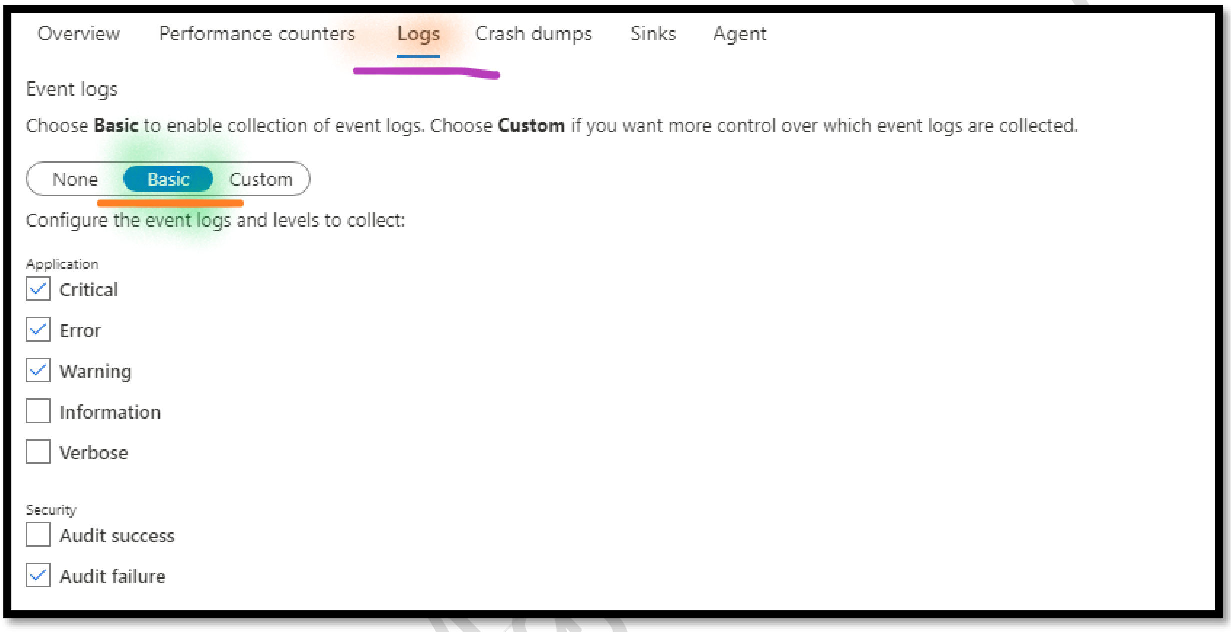
■ Performance counter	Sample rate (seconds)
☑ CPU	60
☑ Memory	60
☑ Disk	60
☑ Network	60
□ ASP.NET	60
□ SQL Server	60

Step 3: View the Logs

30. From Azure portal, go to left side, select **Virtual machines**
31. Select & Open **Az204-11-VM** virtual machine
32. Select **Diagnostic settings** under **monitoring**
33. Select **Performance counters**

Note: **Review**, the available event log collection options.

Note: By default, log collection includes critical, error, and warning entries from the Application Log and System log, as well as Audit failure entries from the Security log. Here as well you can switch to the Custom view for more detailed configuration settings.



Event logs

Choose **Basic** to enable collection of event logs. Choose **Custom** if you want more control over which event logs are collected.

None [✓ Basic] Custom

Configure the event logs and levels to collect:

Application

☑ Critical

☑ Error

☑ Warning

□ Information

□ Verbose

Security

□ Audit success

☑ Audit failure

Step 4: Enable Sink

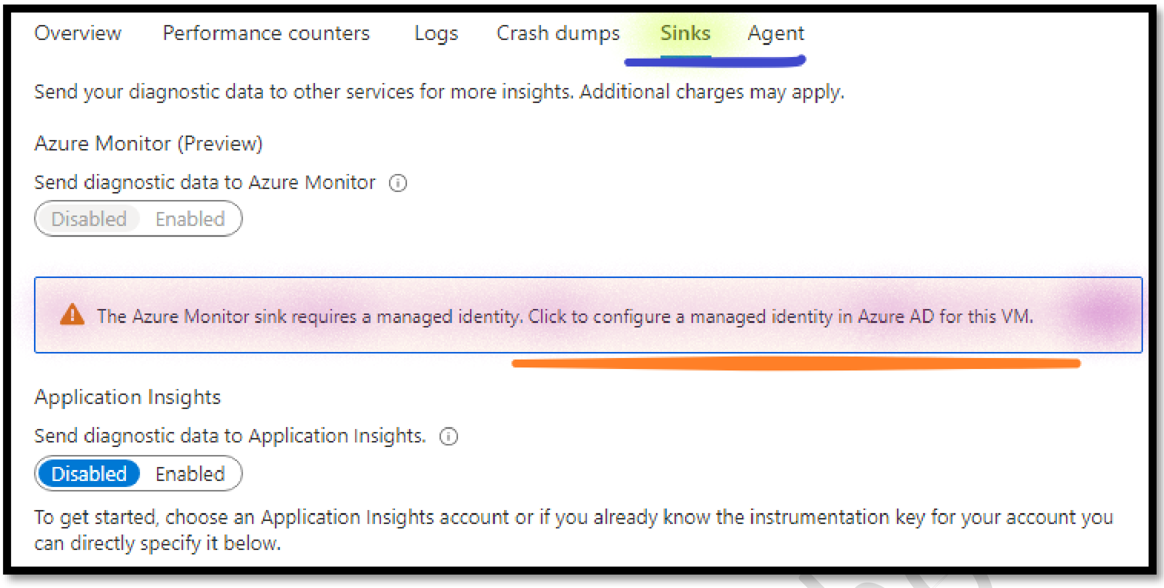
34. From Azure portal, go to left side, select **Virtual machines**

35. Select & Open **Az204-11-VM** virtual machine

36. Select **Diagnostic settings** under **monitoring**

37. Select **Sinks**

    a. Select, **Select Click to configure a managed identity in Azure AD for this VM**.



Send your diagnostic data to other services for more insights. Additional charges may apply.

Azure Monitor (Preview)

Send diagnostic data to Azure Monitor

Disabled Enabled

The Azure Monitor sink requires a managed identity. Click to configure a managed identity in Azure AD for this VM.

Application Insights

Send diagnostic data to Application Insights.

Disabled Enabled

To get started, choose an Application Insights account or if you already know the instrumentation key for your account you can directly specify it below.

i. Select **System Identity**.

ii. Select **On**.

iii. Select **Save**.

38. From Azure portal, go to left side, select **Virtual machines**

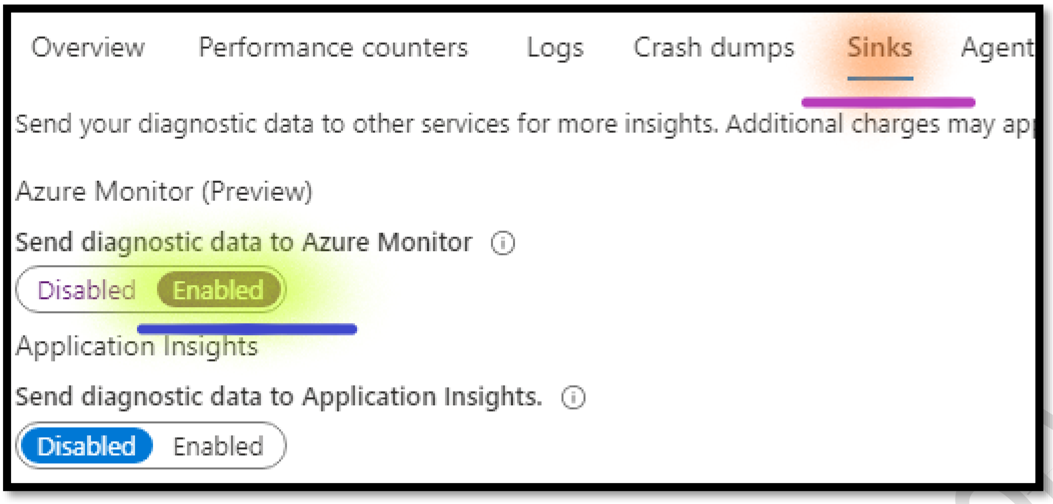
39. Select & Open **Az204-11-VM** virtual machine

40. Select **Diagnostic settings** under **monitoring**

41. Select **Sinks**

a. **Send diagnostic data to Azure Monitor**: Select **Enabled**

b. **Send diagnostic data to Application Insights**: Select **Disabled**.



Send your diagnostic data to other services for more insights. Additional charges may ap

Azure Monitor (Preview)

Send diagnostic data to Azure Monitor: Disabled [✓ Enabled]

Application Insights

Send diagnostic data to Application Insights.: [✓ Disabled] Enabled

c. Select **Save**.

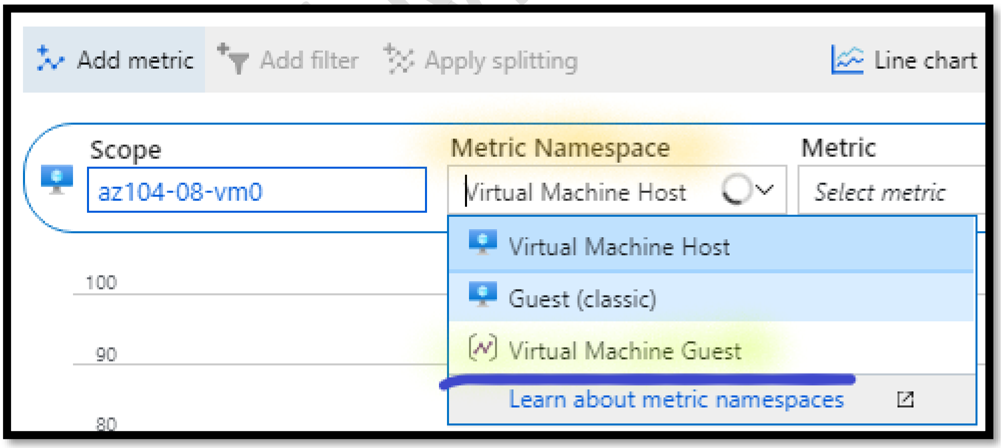
Step 5: View the Guest Level Monitoring

42. From Azure portal, go to left side, select **Virtual machines**

43. Select & Open **Az204-11-VM** virtual machine

44. Select **Metrics** under **monitoring**

a. **Metric namespace**: Dropdown and Select **Virtual Machine Guest**.



Scope: az104-08-vm0

Metric Namespace: Virtual Machine Host

Metric: Select metric

Note: If yo don't see the Virtual machine Guest option, Go to the Sinks and Disable it and re-enable it.

b. **Metric: Review** the list of **available metrics**.

Note: The list includes additional guest-level metrics not available when relying on the host-level monitoring only.

i. **Metric**: Dropdown and Select **Memory/ Available Bytes**.

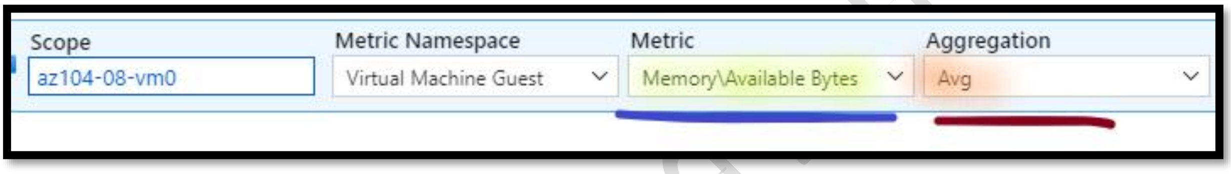
ii. **Aggregation**: Dropdown and Select **Avg**.

c. ***Go to right***, Click on **Local time**.

i. **Time range**: Select **Last 30 minutes**.

ii. **Time granularity**: Dropdown and Select **1 minute**.

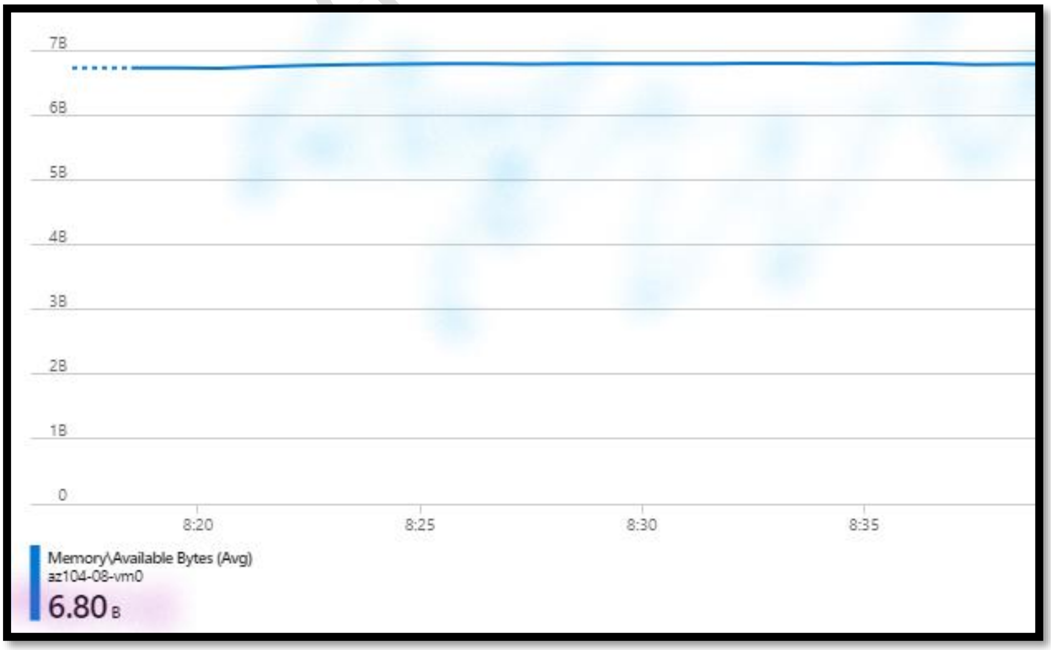
iii. Select **Apply**.



Scope	Metric Namespace	Metric	Aggregation
az104-08-vm0	Virtual Machine Guest	Memory\Available Bytes	Avg

Note: **Review**, the resulting results. You get the available memory.

Note: If you get **Error retrieveing data**, **Wait**, for mnts. and Refresh your Screen to view the metrics.



Task 5: Configure Azure Alert

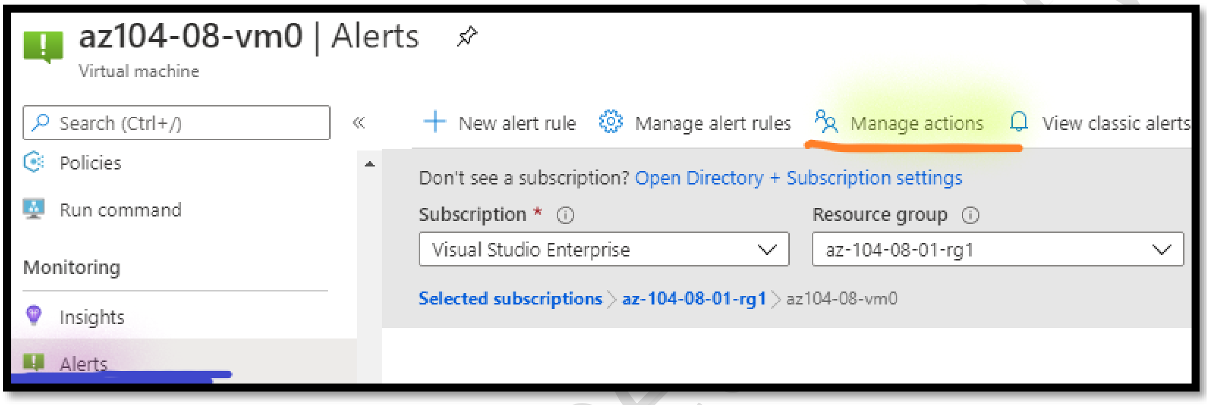
Step 1: Create Action Group

45. From Azure portal, go to left side, select **Virtual machines**

46. Select & Open **Az204-11-VM** virtual machine

47. Select **Alerts** under **monitoring**

48. Click **Manage actions**



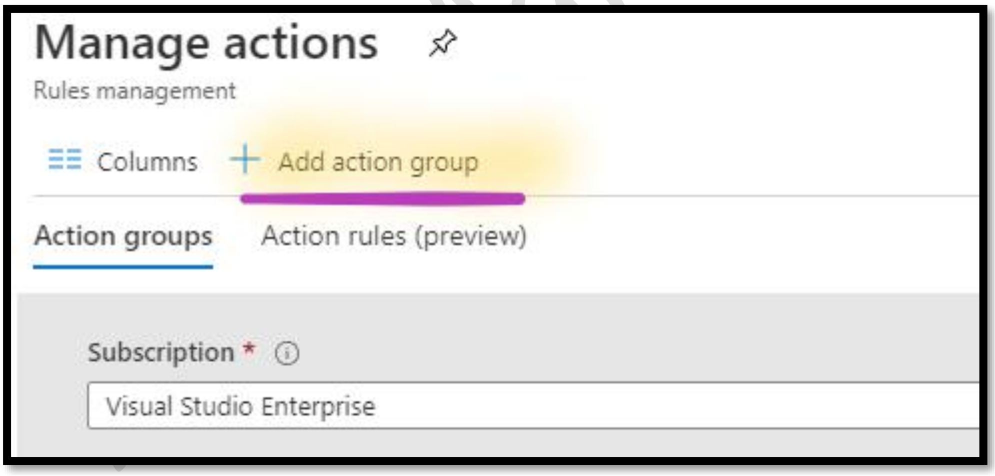
Don't see a subscription? Open Directory + Subscription settings

Subscription * : Visual Studio Enterprise

Resource group : az-104-08-01-rg1

Selected subscriptions > az-104-08-01-rg1 > az104-08-vm0

49. Select **Add action group**



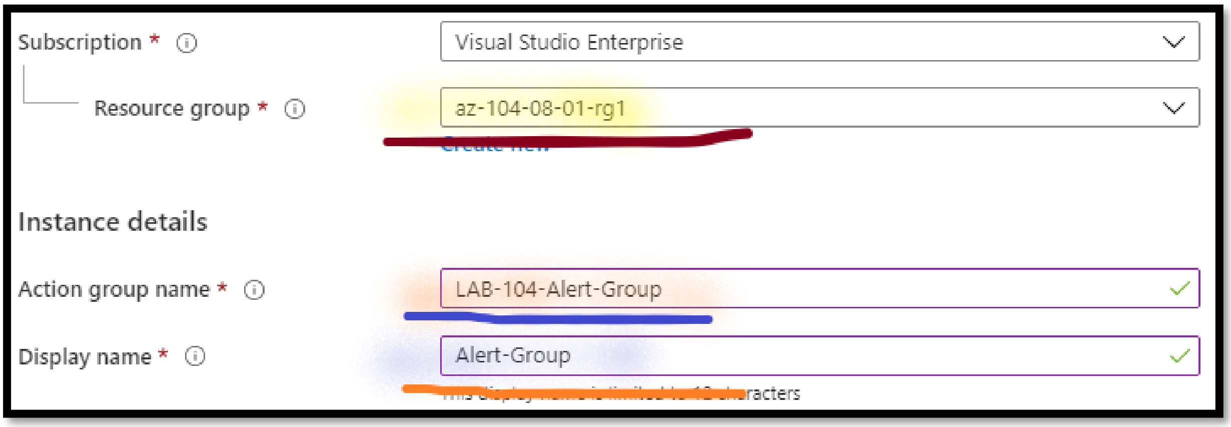
Subscription * : Visual Studio Enterprise

a. **Subscription**: Select your **Default subscription**

b. **Resource group**: Dropdown and Select **AZ-204-11-01-RG**

c. **Action group name**: Write **LAB-204-Alert-Group**

d. **Display name**: Write **Alert-Group**



Subscription * ⓘ Visual Studio Enterprise

Resource group * ⓘ az-104-08-01-rg1

Instance details

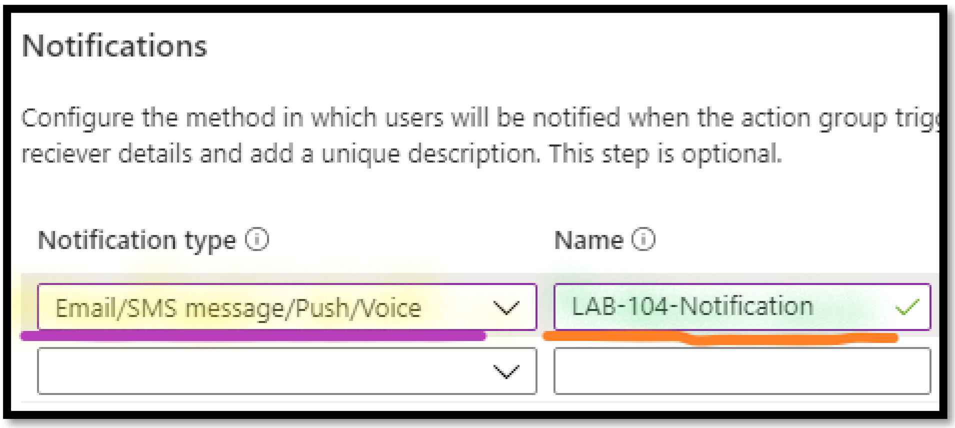
Action group name * ⓘ LAB-104-Alert-Group ✓

Display name * ⓘ Alert-Group ✓

e. Select **Next: Notification**

f. **Notification type**: Dropdown and Select **Email/SMS message/ Push/ Voice**

1) **Name**: Write **LAB-104-Notification**



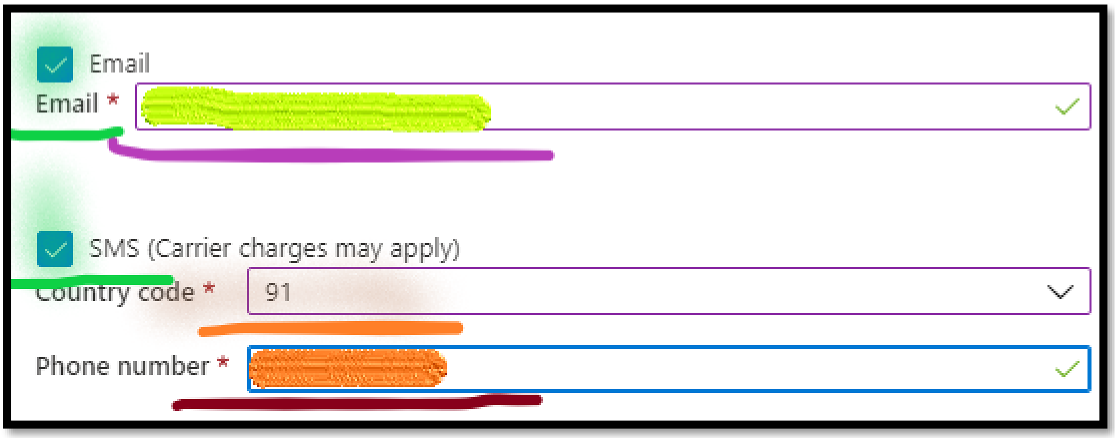
Notifications

Configure the method in which users will be notified when the action group trig reciever details and add a unique description. This step is optional.

Notification type ⓘ	Name ⓘ
Email/SMS message/Push/Voice	LAB-104-Notification ✓

- **Email:** Enable **email**
  i. Provide **your email id**

- **SMS:** Enable **SMS**
  i. Select your **country code**
  ii. Provide **your mobile no.**



☑ Email

Email * [redacted]

☑ SMS (Carrier charges may apply)

Country code * 91

Phone number * [redacted]

2) Press **Ok**

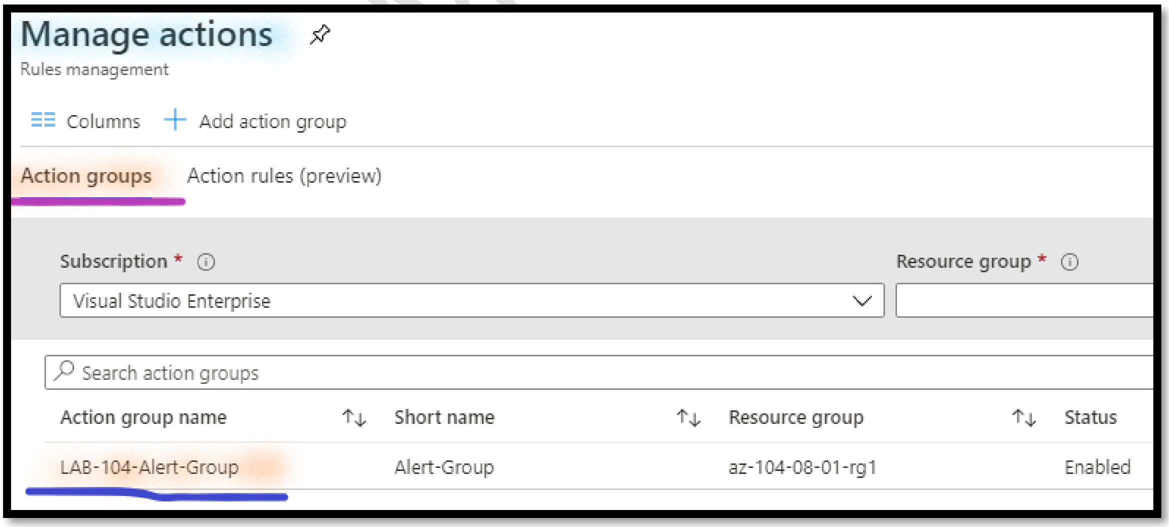
g. Select **Next: Actions**

h. Select **Next: Tags**

i. Select **Next: Review + Create**

j. Select **Create**

Note: You can see your action group.



Manage actions

Rules management

Subscription * Visual Studio Enterprise

Resource group *

Search action groups

Action group name	Short name	Resource group	Status
LAB-104-Alert-Group	Alert-Group	az-104-08-01-rg1	Enabled

Note: If you are unable to view action group, it takes few mnts. to view the action group.
Don't wait, go to the next step.

Note: You can receive e-mail /sms that **You ve been added to an Azure Monitor action group**.

Step 2: Create Alert

50. From Azure portal, go to left side, select **Virtual machines**

51. Select & Open **Az204-11-VM** virtual machine

52. Select **Alerts** under **monitoring**

53. Select **New Alert rule**

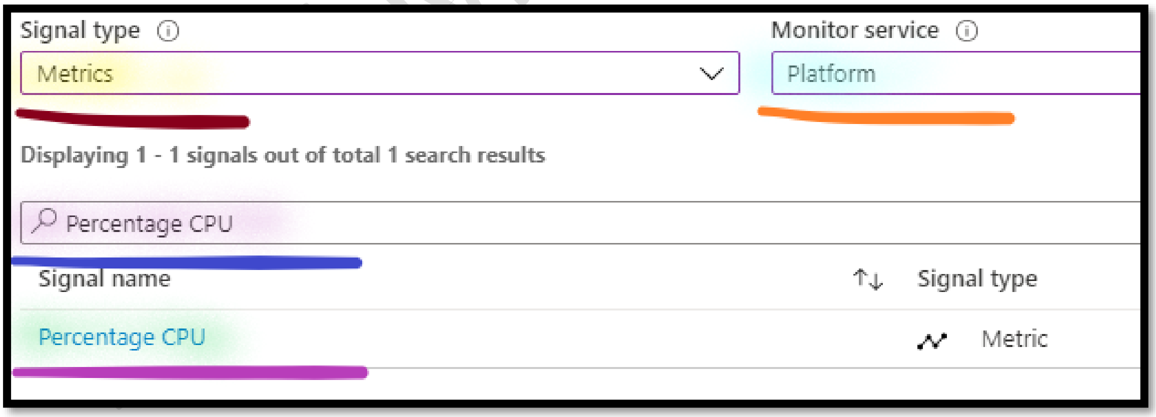
Note: You can see the virtual machine **az204-11-vm** is already added under resource.

54. **Condition**: Click on **Add Condition**

  a. **Signal type**: Dropdown & Select **Metrics**

  b. **Monitor service**: Dropdown & select **Platform**

  c. **Signal name:** Search and Select **Percentage CPU**



Signal type: Metrics

Monitor service: Platform

Displaying 1 - 1 signals out of total 1 search results

Percentage CPU

Signal name	Signal type
Percentage CPU	Metric

Note: You can see new blade to configure signal logic.

55. In **Alert logic section**, configure:

  a. **Threshold**: Select **Static**

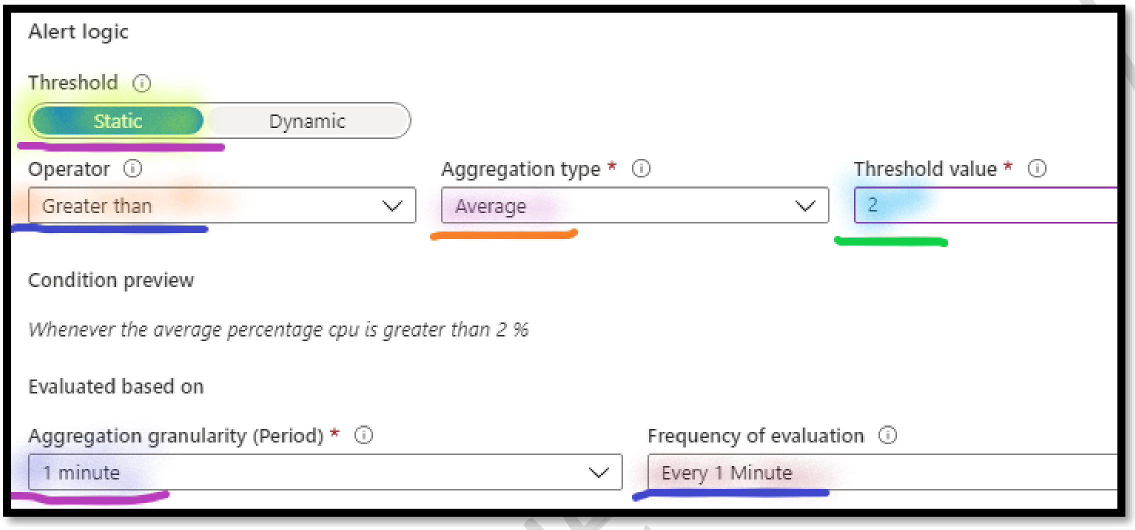
b. **Operator**: Select **Greater than**

c. **Aggregation type**: Select **Average**

d. **Threshold value**: Write **2**

e. **Aggregation granularity**: Dropdown and Select **1 Minute**

f. **Frequency of evaluation**: Dropdown and Select **Every 1 Minute**



Alert logic

Threshold ⓘ

Operator ⓘ: Greater than

Aggregation type * ⓘ: Average

Threshold value * ⓘ: 2

Condition preview

Whenever the average percentage cpu is greater than 2 %

Evaluated based on

Aggregation granularity (Period) * ⓘ: 1 minute

Frequency of evaluation ⓘ: Every 1 Minute

g. select **Done**

56.In **Action group section**, configure:

a. Click on **Add Action group**, under **actions**

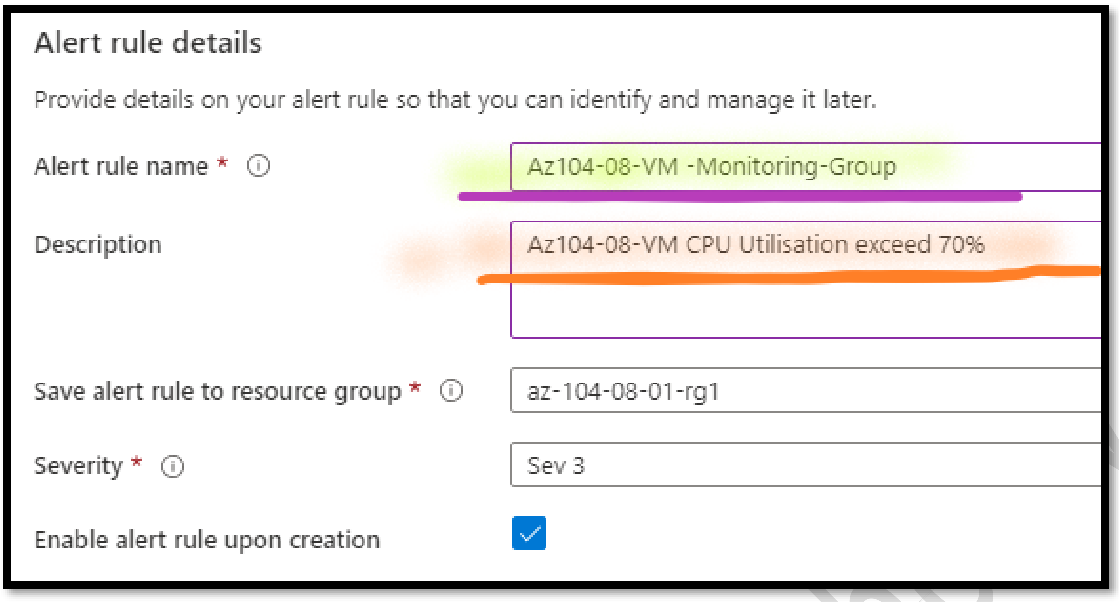
b. Select **LAB-204-Alert-Group**

c. Click **Select**

57.In **Alert rule details section**, configure:

a. **Alert rule name**: Write **Az204-11-VM -Monitoring-Group**

b. **Description**: Write **Az204-11-VM CPU Utilisation exceed 2%**



Alert rule details

Provide details on your alert rule so that you can identify and manage it later.

Alert rule name * ⓘ Az104-08-VM -Monitoring-Group

Description Az104-08-VM CPU Utilisation exceed 70%

Save alert rule to resource group * ⓘ az-104-08-01-rg1

Severity * ⓘ Sev 3

Enable alert rule upon creation ☑

Note: Leave other settings as default.

c. Click on **Create alert rule**

Step 3: Verify Alert rule

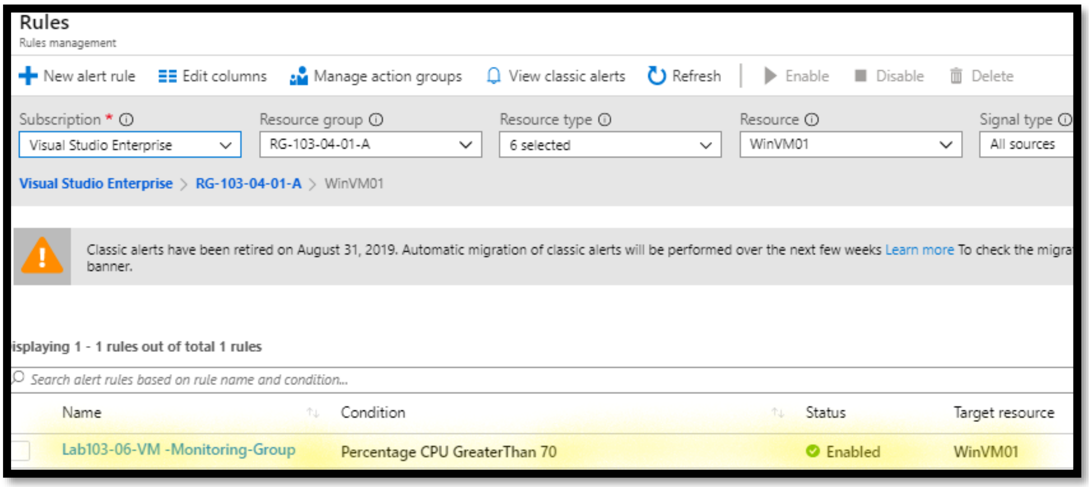
58. From Azure portal, go to left side, select **Virtual machines**

59. Select & Open **Az204-11-VM** virtual machine

60. Select **Alerts** under **monitoring**

61. Select **Manage Alert rule**

Note: You can see the newly created alert rule.



Rules
Rules management

Subscription * Visual Studio Enterprise
Resource group RG-103-04-01-A
Resource type 6 selected
Resource WinVM01
Signal type All sources

Visual Studio Enterprise > RG-103-04-01-A > WinVM01

Classic alerts have been retired on August 31, 2019. Automatic migration of classic alerts will be performed over the next few weeks Learn more To check the migra
banner.

isplaying 1 - 1 rules out of total 1 rules

Search alert rules based on rule name and condition...

Name	Condition	Status	Target resource
Lab103-06-VM -Monitoring-Group	Percentage CPU GreaterThan 70	Enabled	WinVM01

Step 4: Stress VM CPU for Alert

62. Login to **Az204-11-VM** windows virtual machine via **RDP**.

63. Go to **Start** menu, right click on **Start** & **Run**.

    a. In the **open**, **write** **cmd**

    b. **Run** the following to initiate the infinite loop that should increase the CPU utilization above the threshold of the newly created alert rule. **From** the **command line interpreter**, run the **following**:

```
for /l %a in (0,0,1) do echo a
```

Step 5: Review the CPU metrics

64. From Azure portal, go to left side, select **Virtual machines**

65. Select & Open **Az204-11-VM** virtual machine

66. Select **Metrics** under **monitoring**

    a. In the **Metric drop-down list**, **review** the list of available metrics.

        i. **Metric**: Dropdown and Select **Percentage CPU**.

        ii. **Aggregation**: Dropdown and Select **Avg**.

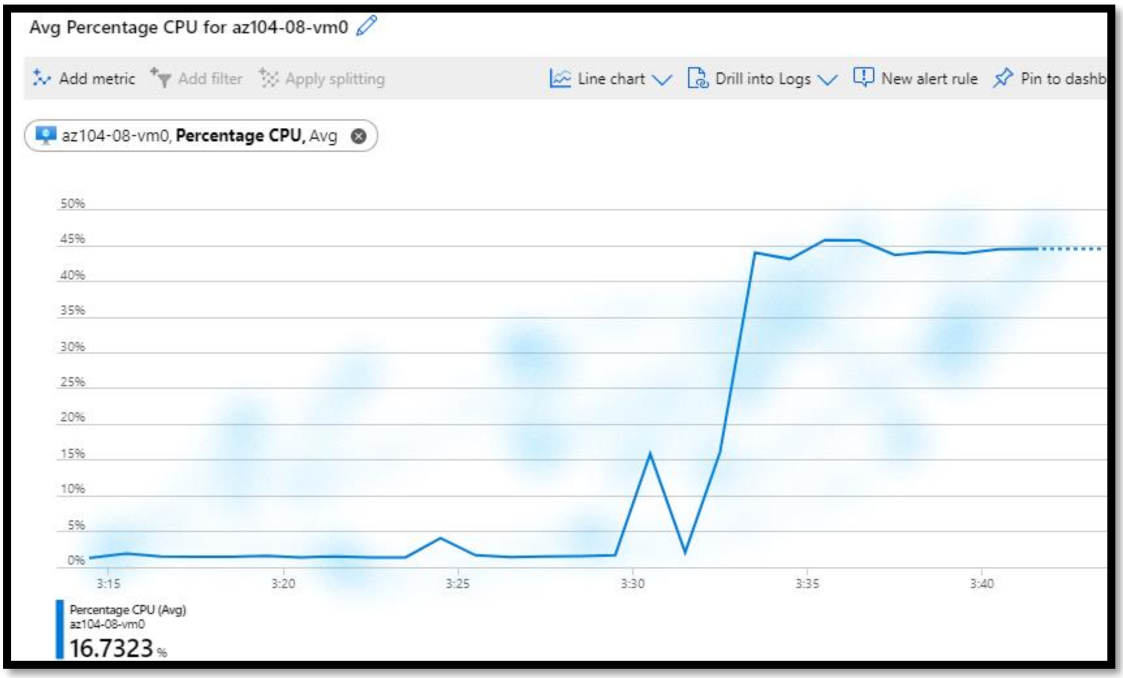
    b. **Go to the right**, Click on **Local time**.

i. **Time range**: Select **Last 30 minutes**.

ii. **Time granularity**: Dropdown and Select **1 minute**.

iii. Select **Apply**.

Note: You can see the CPU metrics going beyond threshold. Keep Refresh to check the current CPU status.



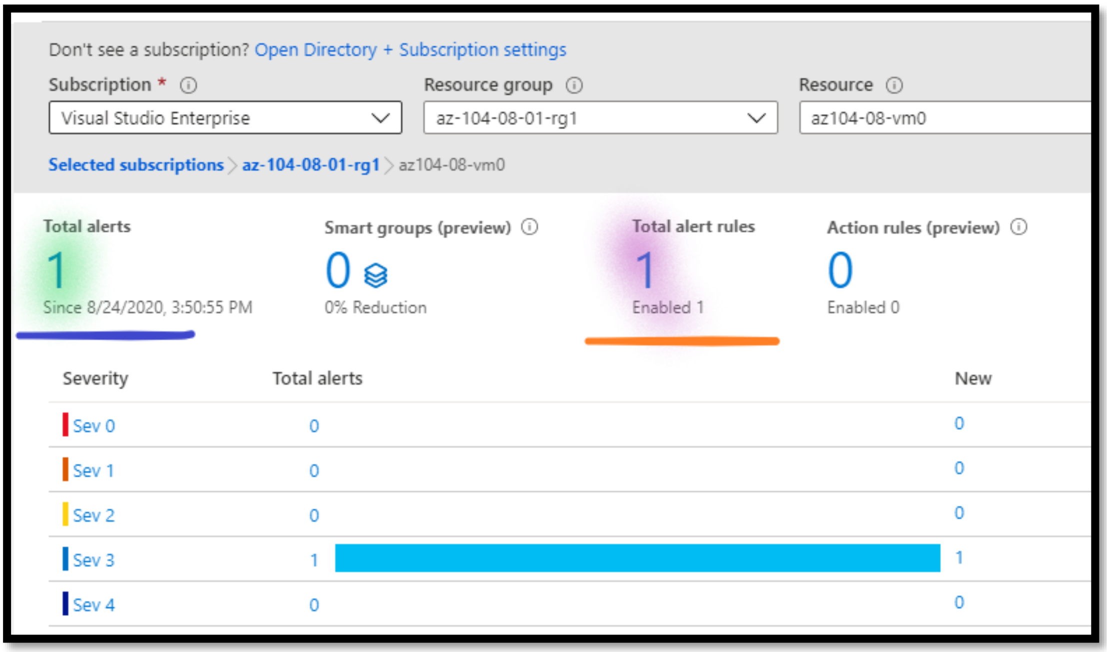
Step 6: Monitor Alert

67.From Azure portal, go to left side, select **Virtual machines**

68.Select & Open **Az204-11-VM** virtual machine

69.Select **Alerts** under **monitoring**

Note: First alert takes **~15 mnts**., you will see the triggered alert details.



Don't see a subscription? Open Directory + Subscription settings

Subscription * : Visual Studio Enterprise

Resource group: az-104-08-01-rg1

Resource: az104-08-vm0

Selected subscriptions > az-104-08-01-rg1 > az104-08-vm0

Total alerts: 1 — Since 8/24/2020, 3:50:55 PM

Smart groups (preview): 0 — 0% Reduction

Total alert rules: 1 — Enabled 1

Action rules (preview): 0 — Enabled 0

Severity	Total alerts	New
Sev 0	0	0
Sev 1	0	0
Sev 2	0	0
Sev 3	1	1
Sev 4	0	0

70. You will receive **email** and **sms** for your azure monitor alert rule.

Note: **Don't wait**, go to the next step.

Task 6: Review Azure Log Analytics

Step 1: Review Azure Log Analytics functionality

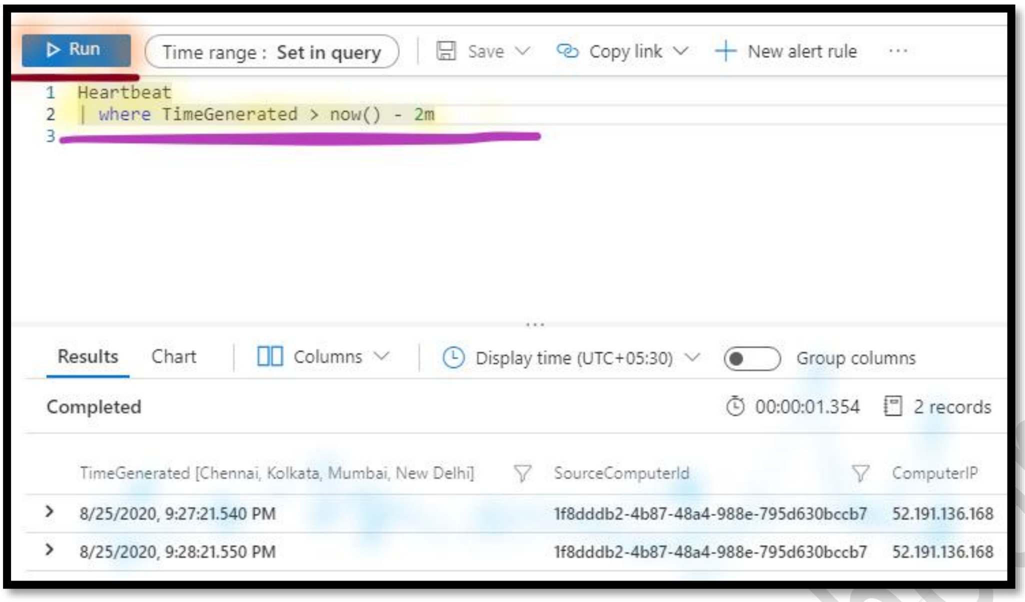
71. From Azure portal, go to left side, select **Virtual machines**

72. Select & Open **Az204-11-VM** virtual machine

73. Select **Logs** under **monitoring**

74. In the **query window**, paste the following query to see all heartbeats over the last two minutes and click **Run**:

```
Heartbeat
| where TimeGenerated > now() - 2m
```



```
Heartbeat
| where TimeGenerated > now() - 2m
```

Completed 00:00:01.354 2 records

TimeGenerated [Chennai, Kolkata, Mumbai, New Delhi]	SourceComputerId	ComputerIP
8/25/2020, 9:27:21.540 PM	1f8dddb2-4b87-48a4-988e-795d630bccb7	52.191.136.168
8/25/2020, 9:28:21.550 PM	1f8dddb2-4b87-48a4-988e-795d630bccb7	52.191.136.168

Note: You can review the result.

Task 6: Review Azure Activity Log

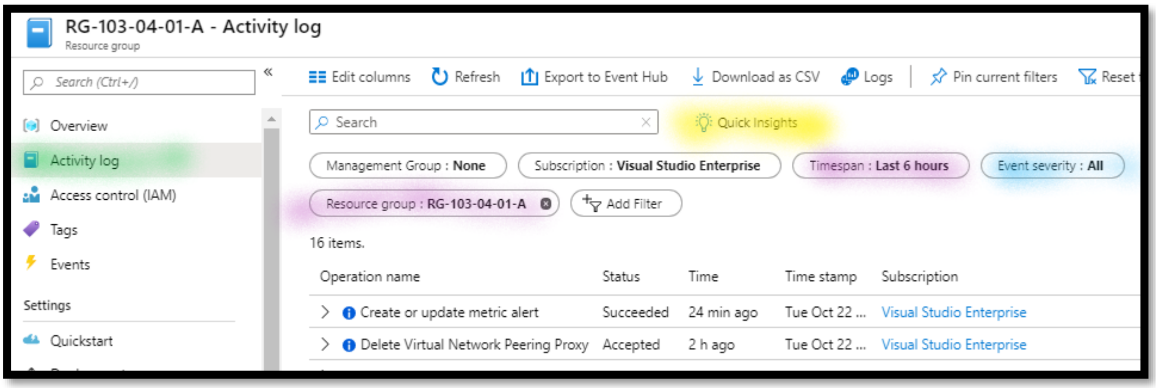
Step 1: Query Activity Logs

75. To view the **activity logs** through the portal, select resource group **AZ-204-11-01-RG**

76. Select **Activity Log**

    a. You will see **summary of recent operations**. A default set of filters is applied to the operations.

    b. To quickly run a pre-defined set of filters, select **Quick Insights**



Management Group : None | Subscription : Visual Studio Enterprise | Timespan : Last 6 hours | Event severity : All | Resource group : RG-103-04-01-A

16 items.

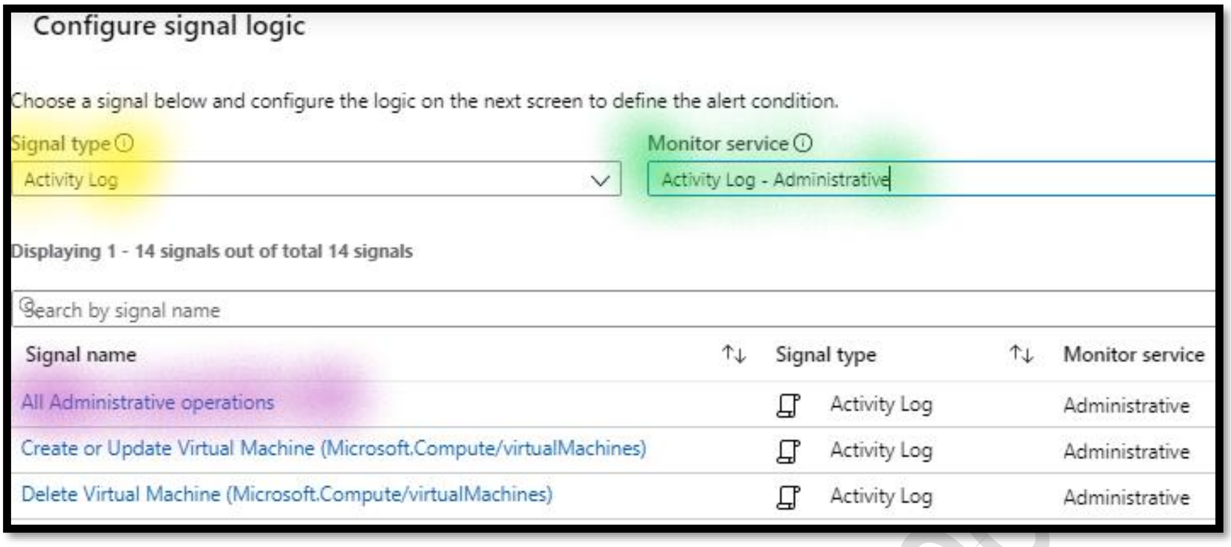
Operation name	Status	Time	Time stamp	Subscription
Create or update metric alert	Succeeded	24 min ago	Tue Oct 22 ...	Visual Studio Enterprise
Delete Virtual Network Peering Proxy	Accepted	2 h ago	Tue Oct 22 ...	Visual Studio Enterprise

c. Select one of the options. For example, select **Failed deployments** to see errors from deployments.

Note: Use filters to get more details.

Step 2: Create Activity Log Alert

77. From Azure portal, go to left side, select **Resource group**
78. Open resource group **AZ-204-11-01-RG**
79. Click **Alert** under monitoring
80. Select **New Rule Alert**
81. Click on **Select resource**, under Resource
    a. **Filter by subscription**: Dropdown & select **default subscription**
    b. **Filter by resource type**: Dropdown & select **Virtual machines**
    c. Under **resource** select your **Az204-11-VM** virtual machine
    d. Select **Done**
82. Click on **Select conditions**, under **Conditions**
    a. **Signal type**: Dropdown & Select **Activity log**
    b. **Monitor service**: Dropdown & select **Activity log– Administrative**
    c. **Signal name:** Select **All Administrative operations**



Configure signal logic

Choose a signal below and configure the logic on the next screen to define the alert condition.

Signal type: Activity Log

Monitor service: Activity Log - Administrative

Displaying 1 - 14 signals out of total 14 signals

Search by signal name

Signal name	Signal type	Monitor service
All Administrative operations	Activity Log	Administrative
Create or Update Virtual Machine (Microsoft.Compute/virtualMachines)	Activity Log	Administrative
Delete Virtual Machine (Microsoft.Compute/virtualMachines)	Activity Log	Administrative

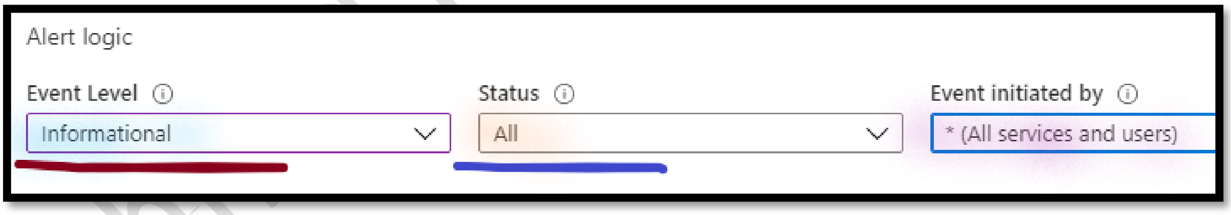
Note: New blade of Configure signal logic gets open.

i. In **Alert logic** section, configure:

1) **Event level**: Dropdown and Select **Informational**.

2) **Status**: Dropdown and Select **All**.

Note: Leave other settings as default.



Alert logic

Event Level: Informational

Status: All

Event initiated by: * (All services and users)

3) Select **Done**

d. Click on **Select action group**, under **Action group**

i. Select **LAB-204-Alert-Group**

ii. Click **Select**

e. In **Alert rule details** section, configure:

i. **Alert rule name**: Write **AZ204-11-VM-State-Monitoring-Group**

ii. **Description**: Write **AZ204-11-VM State Change**

Note: Leave other settings as default.

iii. Click on **Create alert rule**

Step 3: Verify Alert rule

83. From Azure portal, go to left side, select **Virtual machines**
84. Select & Open **Az204-11-VM** virtual machine
85. Select **Alerts** under **monitoring**

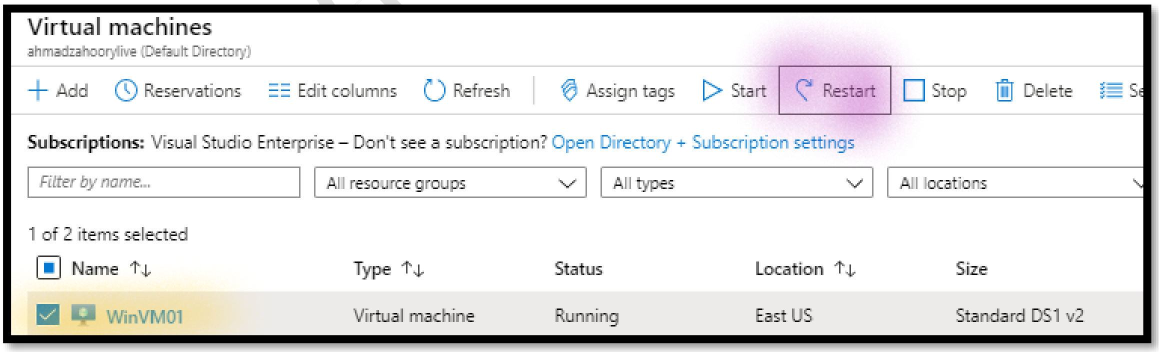
   a. Select **Manage Alert rule**

Note: You can see the newly created alert rule.

Step 4: Change the Virtual machine state

86. From Azure portal, go to left side, select **Resource group**
87. Open resource group **AZ-204-11-01-RG**
88. Select **Az204-11-VM** virtual machine

   a. **Restart** the **Az204-11-VM** virtual machine



Virtual machines

ahmadzahooryive (Default Directory)

Subscriptions: Visual Studio Enterprise – Don't see a subscription? Open Directory + Subscription settings

Filter by name... | All resource groups | All types | All locations

1 of 2 items selected

Name ↑↓	Type ↑↓	Status	Location ↑↓	Size
☑ WinVM01	Virtual machine	Running	East US	Standard DS1 v2

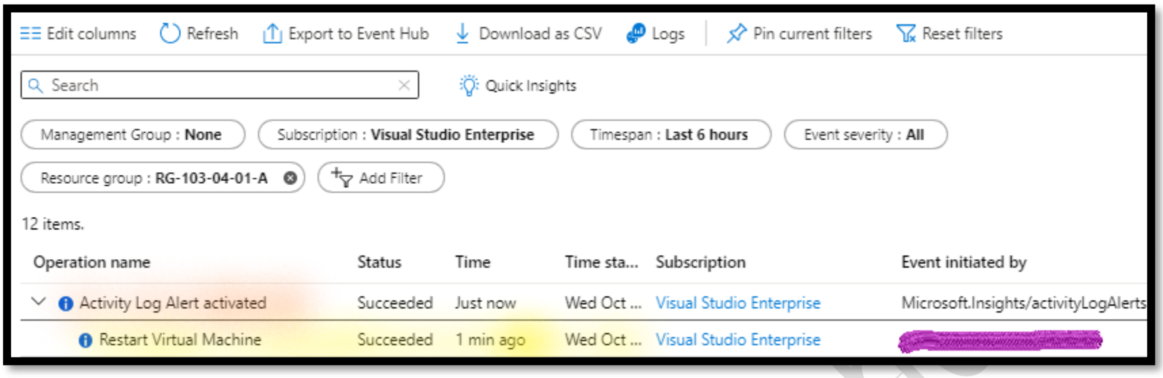
Step 5: Check the Activity Logs

89. To view the **activity logs** through the portal, select resource group **AZ-204-11-01-RG**

   a. Select **Activity Log**

Note: You can **Alert activated** activity log.

b. Expand the **Activity Log Alert activated** to view the **Restart Virtual Machine** log and **event initiated** by



Management Group : None | Subscription : Visual Studio Enterprise | Timespan : Last 6 hours | Event severity : All

Resource group : RG-103-04-01-A

12 items.

Operation name	Status	Time	Time sta...	Subscription	Event initiated by
Activity Log Alert activated	Succeeded	Just now	Wed Oct ...	Visual Studio Enterprise	Microsoft.Insights/activityLogAlerts
Restart Virtual Machine	Succeeded	1 min ago	Wed Oct ...	Visual Studio Enterprise	[redacted]

Note: You will see the triggered alert details.

Task 5: Delete Environment

Step 1: Delete Resource Group

90.Delete **AZ-204-11-01-RG** resource group