

## Monitor VMs using Azure Monitor

### Use Case:

In this walkthrough task we will view the default available monitoring data from within the VM resource data and then from within Azure Monitor. We will view some of the monitoring options available in Azure Monitor, create a Log Analytics workspace, enable Insights in our VM, then review the retrieved data in Azure Monitor. We will enable diagnostic settings in the VM and query and analyze virtual machine logs in Log Analytics workspace and Azure Monitor Logs.

### Steps:

Create Azure resources to allow us to monitor them.

Firstly, we will deploy some resources to Azure to provide us with some resources to manage. If you have resources available from a previous deployment, you can use those instead of deploying new ones.

1. Sign into the Azure Portal and click on the Cloud Shell icon in the top right hand corner



2. The **Cloud Shell** is launched in the bottom of the browser window.

3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** *\*or\** **bash** console.

```
``cli
az group create `
--name monitorgg `
--location westeurope
```

```
PS Azure:\> az group create --name monitorrg --location westeurope
{
  "id": "/subscriptions/7bd726dd-0a34-4060-9168-b1e496983db8/resourceGroups/monitorrg",
  "location": "westeurope",
  "managedBy": null,
  "name": "monitorrg",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": "Microsoft.Resources/resourceGroups"
}
Azure:/
PS Azure:\>
```

4. Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
```cli
az vm create `
--name vmmonitor1 `
--resource-group monitorrg `
--image Win2019Datacenter `
--location westeurope `
--admin-username demouser `
--admin-password demo@pass123
```
```

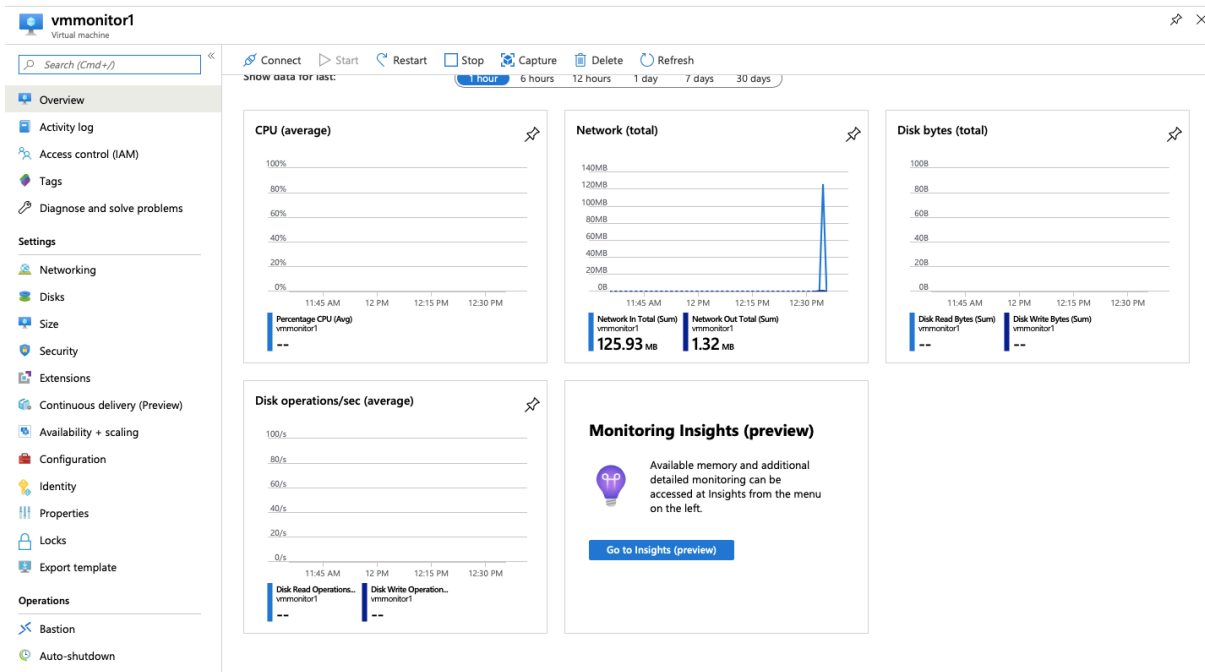
**Note:** The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. You can close the Azure Cloud Shell once it is complete.

```
PS Azure:\> az vm create --name vmmonitor1 --resource-group monitorrg --image Win2019Datacenter --location westeurope --admin-username demouser --admin-passwo
rd demo@pass123
{
  "fqdns": "",
  "id": "/subscriptions/7bd726dd-0a34-4060-9168-b1e496983db8/resourceGroups/monitorrg/providers/Microsoft.Compute/virtualMachines/vmmonitor1",
  "location": "westeurope",
  "macAddress": "00-0D-3A-A8-F8-45",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "13.81.66.168",
  "resourceGroup": "monitorrg",
  "zones": ""
}
Azure:/
```

### View default available monitoring data within the virtual machine resource

1. Go to the resource group you just created i.e. **monitorrg**, then open the virtual machine and go to the **Overview** pane.

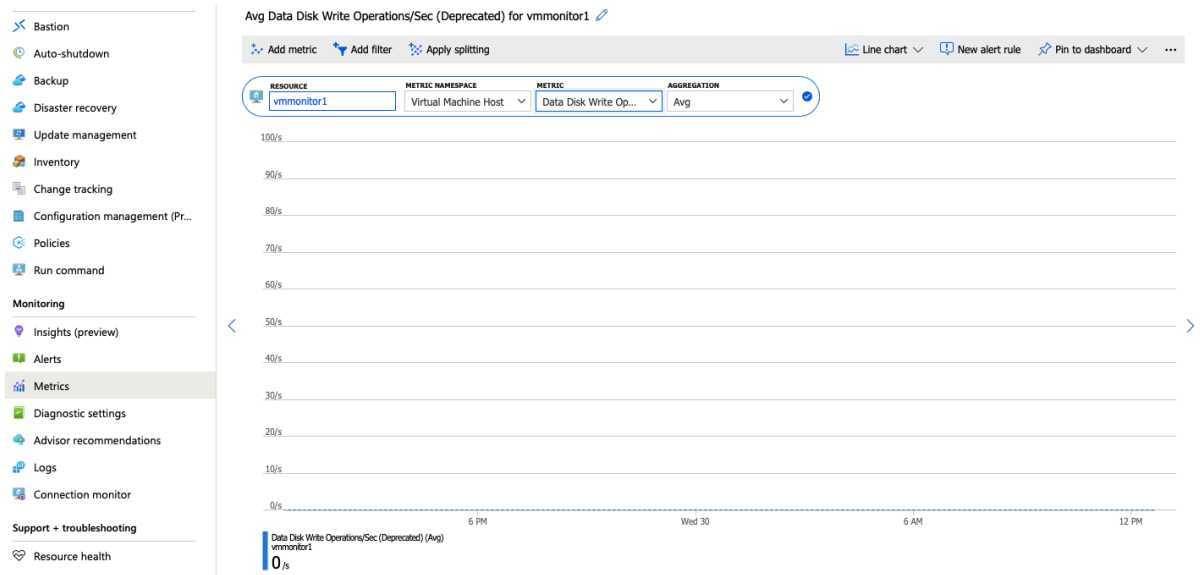
Note the presence of default metric data for **CPU**, **Network**, **Disk bytes** and **Disk operations/sec** present by default in the virtual machine resource.



1. Now click on the **Activity log** and note the presence of operations listed i.e. **Activity logs** record when resources are created or modified. These are subscription level events in Azure, written to an **Activity log**.

Subscription level events in Azure are written to an **Activity log** that you can view from the Azure Monitor menu

2. Now click on the **Monitoring > Metrics** and select the following
  - **Resource:** < your virtual machine i.e. vmmonitor1 >
  - **Metric Namespace:** virtual machine host
  - **Metric:** Disk Write Operations/Sec (or any other metric you wish to view)
  - **Aggregation:** Avg

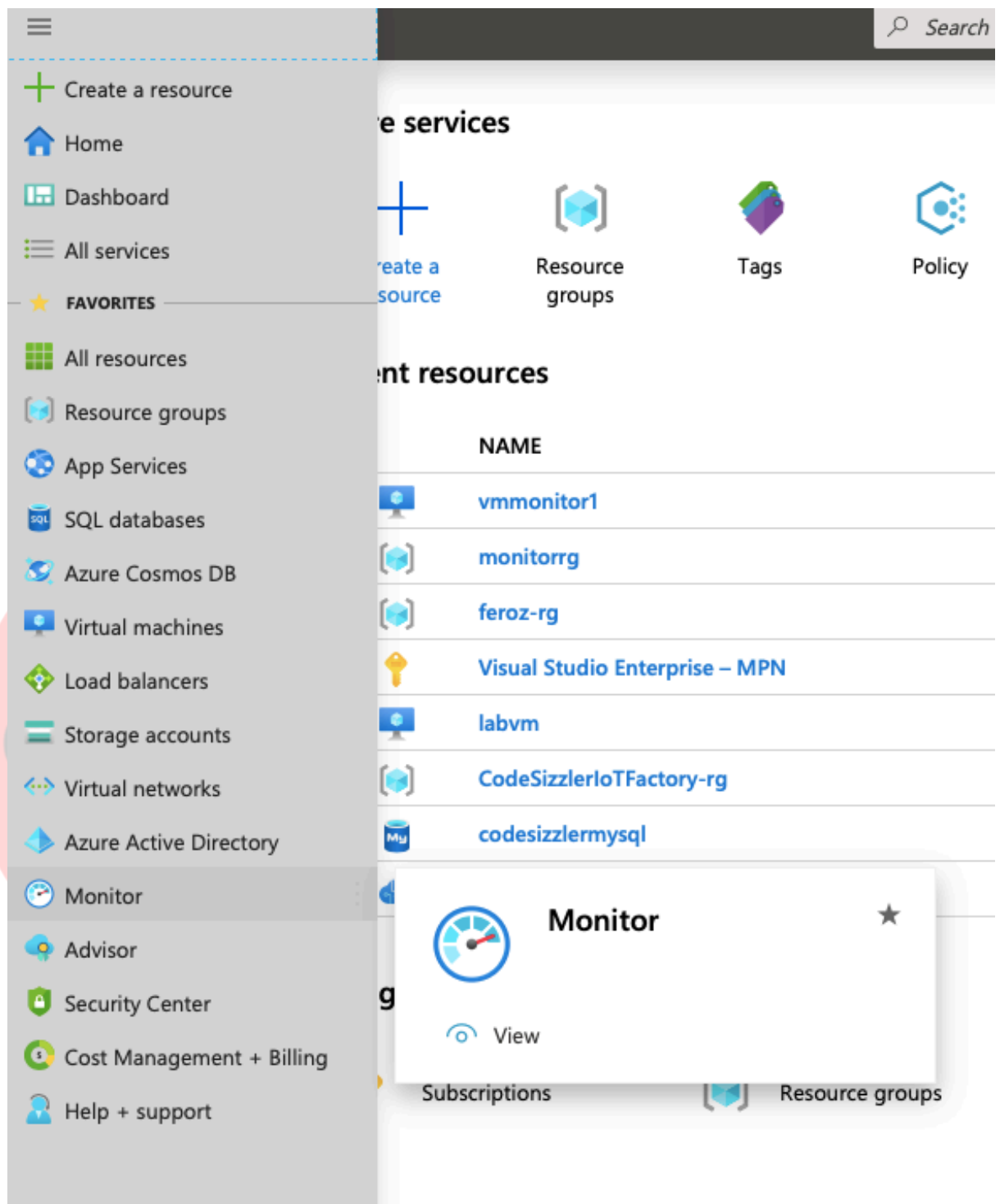


**Note:** **Metric** data tells you how the resource is performing and the resources that it's consuming. Both the **Activity log** and some **Metric** data is available by default and visible from within the resource being monitored i.e. the virtual machine in this case. There not be a lot of data to display for the virtual machine at this point as it has just been installed and no actions have been performed by or to the virtual machine.

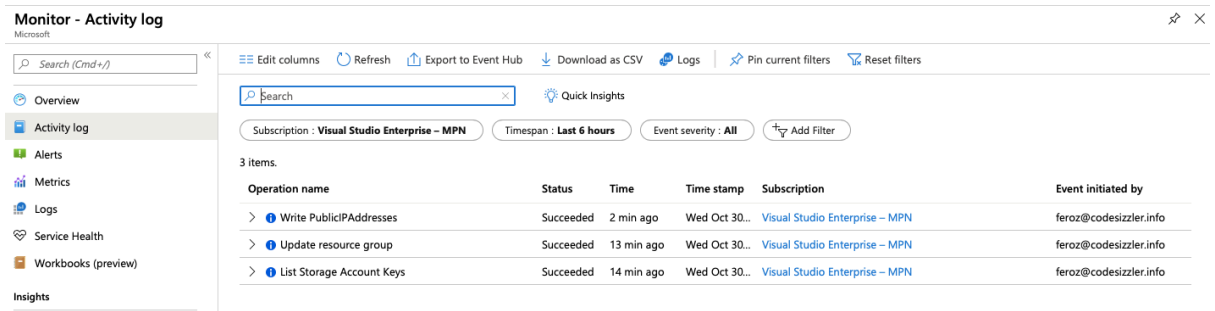
### View default available monitoring data for resources using Azure Monitor

The default metric data is also available for view and analysis via Azure Monitor.

1. In the Azure Portal on the left hand side select **Monitor**

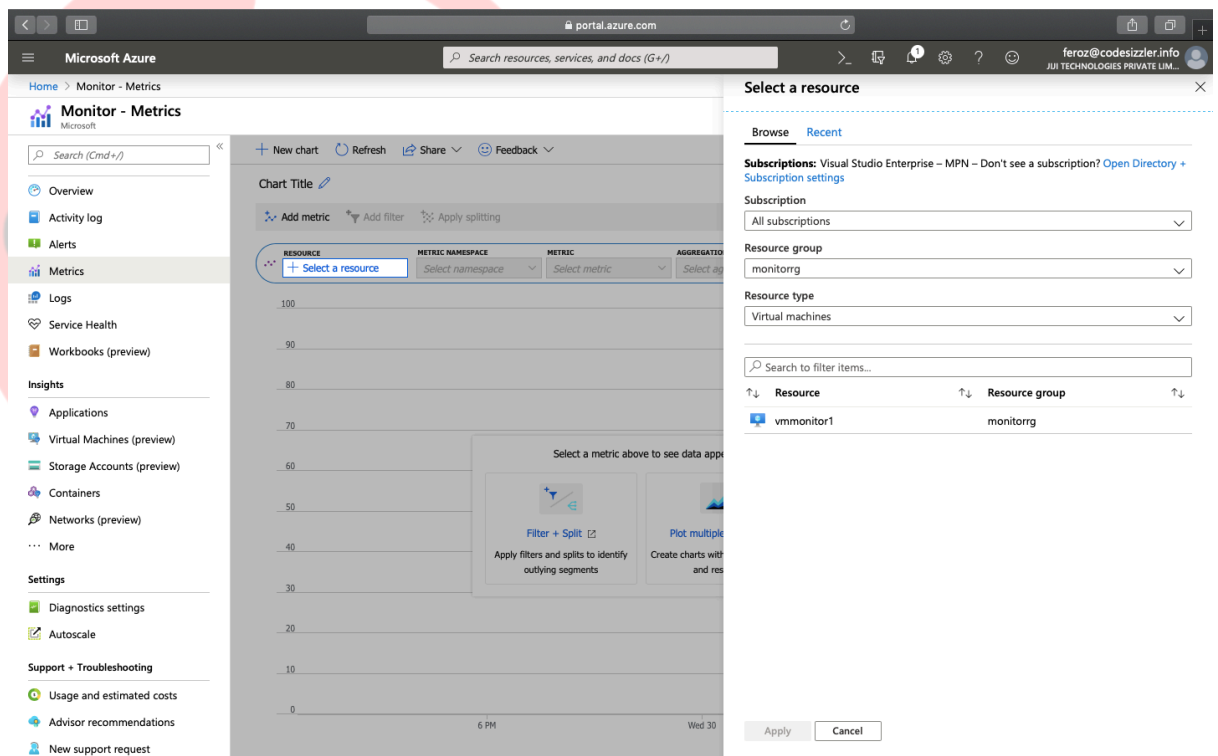


2. Now click on the Activity log and note the presence of operations listed. There are more Activity log operations present here, as they are being pulled at subscription level, not just the single resource level, the virtual machine, that we saw earlier.



3. Now click on the **Metrics**, click **select a resource** and in the resultant **select a resource** pane and fill in the data as below and click **Apply**

- **subscription:** < select your subscription >
- **resource group:** < select the resource group you created earlier i.e. monitorrg >
- **resource type:** All types
- **Resource:** < select the virtual machine i.e. vmmonitor1 >



4. Fill in the remainder of the fields as below

- **Resource:** < your virtual machine i.e. **vmmonitor1** should now be selected >
- **Metric Namespace:** Virtual Machine Host
- **Metric:** Disk Write Operations/Sec
- **Aggregation:** Avg

| RESOURCE   | METRIC NAMESPACE     | METRIC                | AGGREGATION |
|--|----------------------|-----------------------|-------------|
|  vmmonitor1 | Virtual Machine Host | Data Disk Write Op... | Avg         |






**Note:** Both **Activity Log** and **Metric** data is available for resources within the Azure Monitor pane as well as via the individual resource pane. Most resources will write operational information to a diagnostic log that you can forward to different locations. Azure Monitor Logs is a log data platform that collects activity logs and diagnostic logs along with other monitoring data to provide deep analysis across your entire set of resources.

### View Monitoring options within Azure Monitor

In Azure Monitor we are able to monitor all resource types, and we also have available some default scenarios configured for us to use. Take a moment to have a quick look through them. The data available within these requires collection and analysis of logs beyond the default metrics and additional configuration is required.

1. In Azure Monitor go to **Insights > Applications**
2. In Azure Monitor go to **Insights > Virtual machine (Preview)**
3. In Azure Monitor go to **Insights > Container**
4. In Azure Monitor go to **Insights > Network**. This uses the **Network Watcher** service, which is a regional service that enables you to monitor and diagnose conditions at a network level.

### Insights

-  Applications
-  Virtual Machines (preview)
-  Storage Accounts (preview)
-  Containers
-  Networks (preview)
- ... More

**Note:** **Network Watcher** provides for investigating and analyzing areas such as network **Topology**, **Packet capture**, **IP flow**, **Virtual Network Gateway** and **Connection** troubleshooting as well as other areas.

### **Create an Azure Monitor log workspace (also known as Log Analytics workspace)**

Log data collected by Azure Monitor is stored in a Log Analytics workspace. It collects telemetry from a variety of sources and uses the <https://docs.microsoft.com/en-us/azure/kusto/query/> query language used by <https://docs.microsoft.com/en-us/azure/data-explorer/data-explorer-overview> to retrieve and analyze data.

Once the obtained data is stored and organized, we can then monitor, analyze, visualize and create alerts for that data.

We create a *\*workspace\** to allow us to store and process the data collected. Each workspace has its own data repository and configuration, and data sources and solutions are configured to store their data in a particular workspace. You require a Log Analytics workspace if you intend on collecting data from, Azure resources in your subscription, On-premises computers or Diagnostics or log data from Azure storage.

Note: You will see references to **Azure Monitor logs** in documentation as well as **Log Analytics**

1. In the Azure portal, click **All services**, then in the search box type **Log Analytics**. As you begin typing, the list filters based on your input, and select **Log Analytics workspaces**.
2. Click **Create log analytics workspace**. If there is a default workspace present already, click the **+ Add** button instead.
3. In the **Log Analytics workspace** pane enter the following values and click **OK**
  - **Create new:** < select the radio button to indicate Yes >
  - **Log Analytics workspace:** azmon1-lawrkspc
  - **Subscription:** < select your own subscription >
  - **Resource group:** select **Use Existing** and specify the resource group you created earlier that contains your virtual machine i.e. **monitorrg**.
  - **Location:** < a data center near you that supports **Log Analytics** - Not all regions support **Log Analytics**, to see supported regions, go to the page <https://azure.microsoft.com/en-us/global-infrastructure/services/> and search for Azure Monitor from the Search for a product field.
  - **Pricing tier:** Per GB (Standalone) or Per GB (2018), depending on which is available to you - see the page <https://azure.microsoft.com/en-us/pricing/details/monitor/> for more details on pricing.



**Note:** We have now created somewhere for the log data to be collected and organized. It will take 1 to 2 minutes to create the Log Analytics workspace and it should display in the Log Analytics workspace pane once created. You may need to refresh the workspace pane to see it, if it is not present after completion.



## Log Analytics workspace

Create new or link existing workspace

☒ Create New ☐ Link Existing

Log Analytics Workspace \* ⓘ  
azmon2-lawrkspc ✓

Subscription \*  
Visual Studio Enterprise – MPN ▼

Resource group \*  
monitorg ▼  
[Create new](#)

Location \*  
Australia Central ▼

\*Pricing tier

Per GB (2018) >

OK

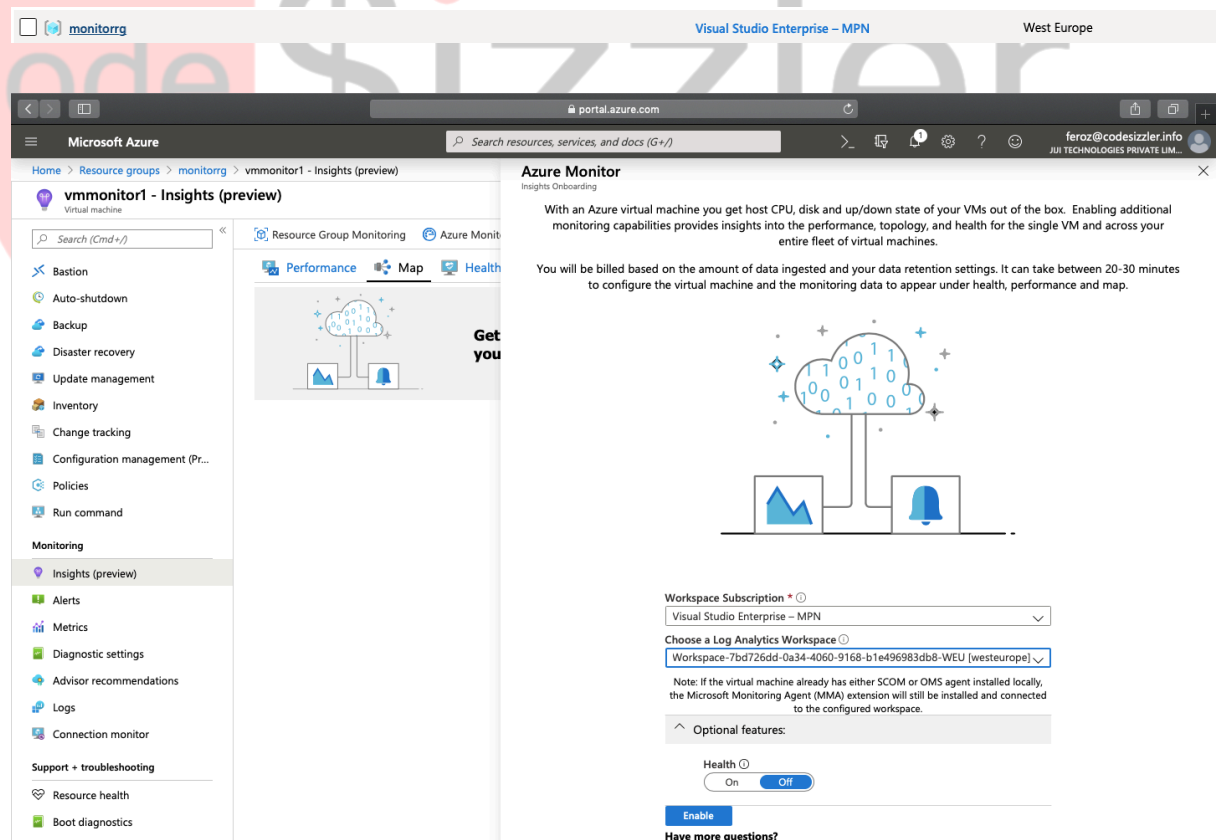
## Enable Insights in the virtual machine resource

To allow us to view monitoring data in Azure Monitor for our virtual machine, outside of the core metrics that are available for CPU, Network and Disk metrics, we need to enable the **Insights** settings within our virtual machine. Enabling these additional monitoring capabilities provides insights into the performance, topology, and health for one or many virtual machines. There are several options available to us to do that for example, using ARM templates, PowerShell or Azure Policy, but we will enable it directly in the resource itself, in the Azure portal.

1. Go to the resource group you created earlier i.e. **monitorrg**, then open the virtual machine i.e. **vmmonitor1**, and go to **Monitoring > Insights (Preview)**. The **Azure Monitor - Insights Onboarding** pane automatically launches read the messages that appear, fill in the fields as below, then click **Enable** and click the **Try Now** button.

- **Workspace subscription:** < your subscription >

- **Choose a Log Analytics Workspace:** azmon2-lawrkspc (the Log Analytics workspace you created earlier)

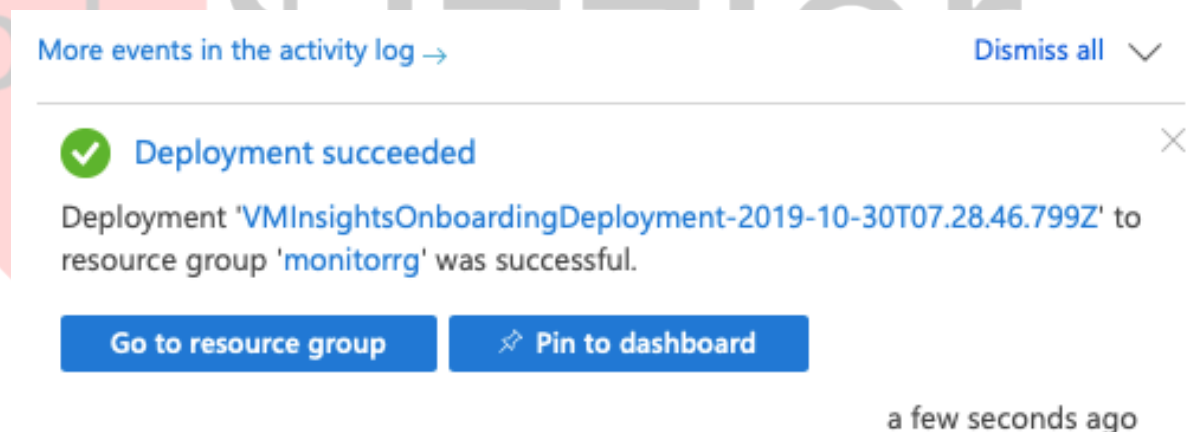


Note: If the **Azure Monitor - Insights Onboarding** pane does not launch automatically, you can click the **Try now** button on the **Insights (preview)** pane to launch it. It will take 2 to 3 minutes to complete the deployment.

2. You will receive a message saying deployment was successful and then a message will display on the **Azure Monitor - Insights Onboarding** stating that **Monitoring data is being collected and routed to Insights and that it can take up to 20 minutes to arrive.....**, additional messages may also display then as the process progresses, stating the **..virtual machine is already collecting data... and to return shortly**, and possibly others. With a simple single VM configuration as ours, it may take approx 10 minutes.

**Note:** As stated, It can take up to 20 minutes for log data to appear, while it is collected and organized. If there is no data present at the moment you can proceed through the next series of tasks below and return to this section later, when it is completed and ready to view the retrieved data.

3. Data will eventually display and be available from within this **Insights (preview)** pane as per the below screenshot.



### View Insights data in Azure Monitor

1. Return to **Azure Monitor** and select **Virtual Machines (preview)** and go to the **Health** tab and ensure your subscription and resource group are selected, then view the health data for the virtual machine.

**Note:** It can take up to 20 minutes for log data to appear, if there is no data present at the moment you can proceed to the next task below and return to this section later, when complete to view the retrieved data. With a simple single VM configuration as ours however, it should take approx 10 minutes.

**Manage Coverage**

Refresh | Configure Workspace | Feedback

**Coverage breakdown**

| Enabled       | Not enabled   | Cannot enable |
|---------------|---------------|---------------|
| 1<br>out of 2 | 0<br>out of 2 | 1<br>out of 2 |

**Subscriptions:** Visual Studio Enterprise – MPN – Don't see a subscription? [Open Directory + Subscription settings](#)

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

| Name       | Insights Status      | Workspace   |
|------------|----------------------|---|
| labvm      | Cannot enable (why?) |   |
| vmmonitor1 | Enabled              | defaultworkspace-7bd726dd-0a34-4060-9168-b1e496983db8-weu |

- Click on the link **View all health criteria** and view the listed health criteria and the state of the various listed components.
- Select the **Performance** and **Map** tabs also, and view the data that's present there. You will need to specify a specific resource group and resource to view data for in those tabs. If you have time you should also click deeper into the various components listed under these tabs to view the data and detail.

**Monitor - Virtual Machines (preview)**

Search (Cmd+J) | Refresh | Provide Feedback

Get Started | Health | **Performance** | Map

Workspace: defaultworkspace-7bd726dd... | Group: <All> | Time range: Last 24 hours | View Workbooks | Azure | Hybrid

Top N Charts | Aggregate Charts | Top N List

**CPU Utilization %** | 15m granularity

Avg | Min | 50th | 90th | **95th** | Max

1.98%

**Available Memory** | 15m granularity

Avg | Max | 50th | 10th | **5th** | Min

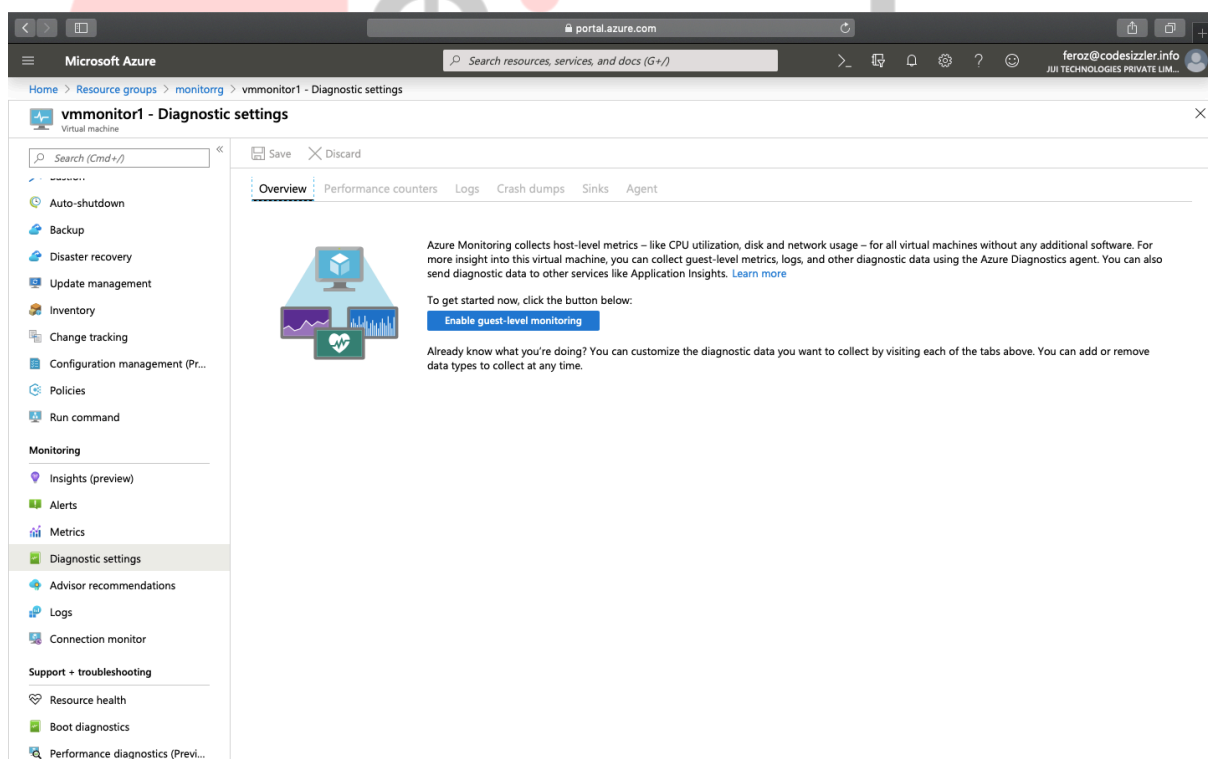
2.3GB

## Enable Diagnostic settings in virtual machine

As mentioned earlier, 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 also collect guest-level metrics, logs, and other diagnostic data using the **Azure Diagnostics agent**. You can also then send diagnostic data to other services like **Application Insights**. We will now enable collection of **Diagnostic data**.

Extend the data you're collecting into the actual operation of the resources by enabling diagnostics and adding an agent to compute resources. This will collect telemetry for the internal operation of the resource and allow you to configure different data sources to collect logs and metrics from Windows and Linux guest operating system.

1. Return to the resource group you created earlier i.e. **monitorrg**, then open the virtual machine i.e. **vmmonitor1**, and go to **Monitoring > Diagnostic settings** and click the **Enable guest-level monitoring** button. It can take approx 2 to 3 minutes to complete.



2. Once enabled, on the **Overview** tab, details about **Performance counters** and **Event Logs**, **Crash Dumps**, **Sinks**, **Agents** etc are listed and you are able to configure them within the VM, to decide what type of data you wish to collect.

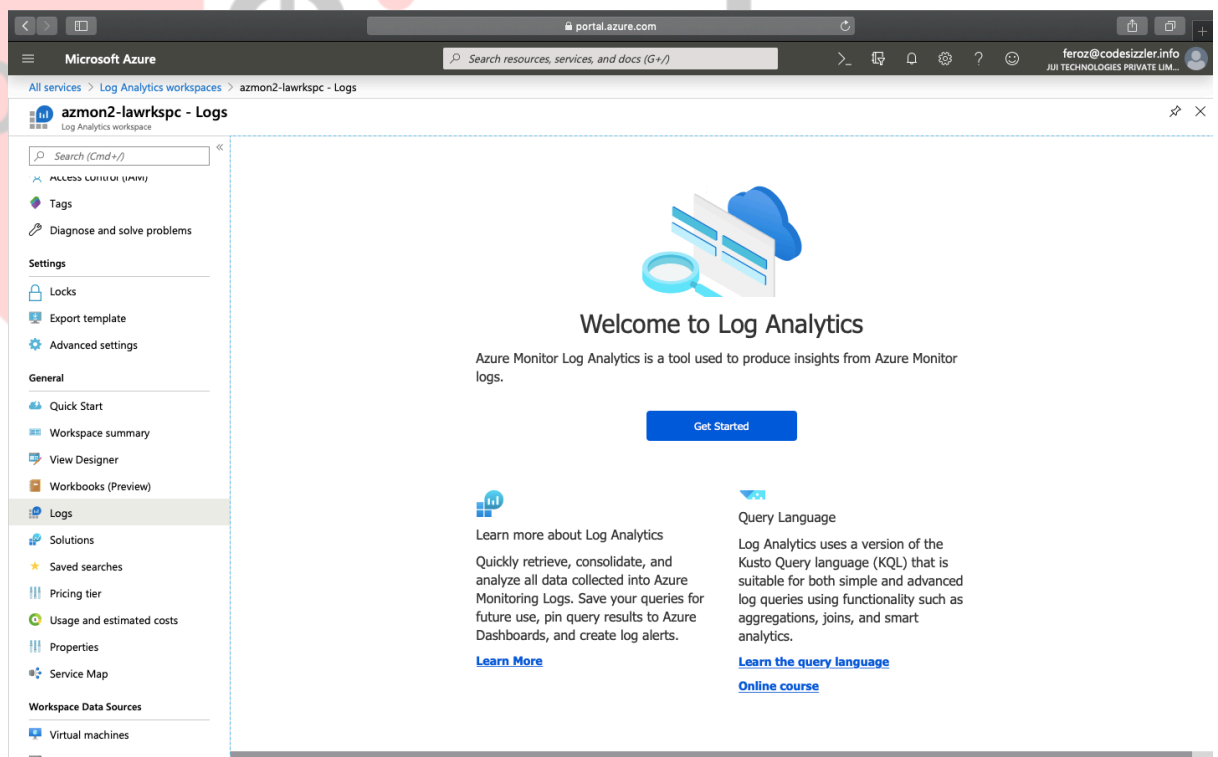
Take a moment to click on the various tabs available i.e. **Performance counters, Logs, Crash Dumps, Sinks** and **Agent** and view their content and the items we can configure and collect.

### Query and Analyze virtual machine logs in Log Analytics workspace and Azure Monitor Logs

Now we will access the Log Analytics workspace and query and analyze some of the log data that we configured earlier to be collected.

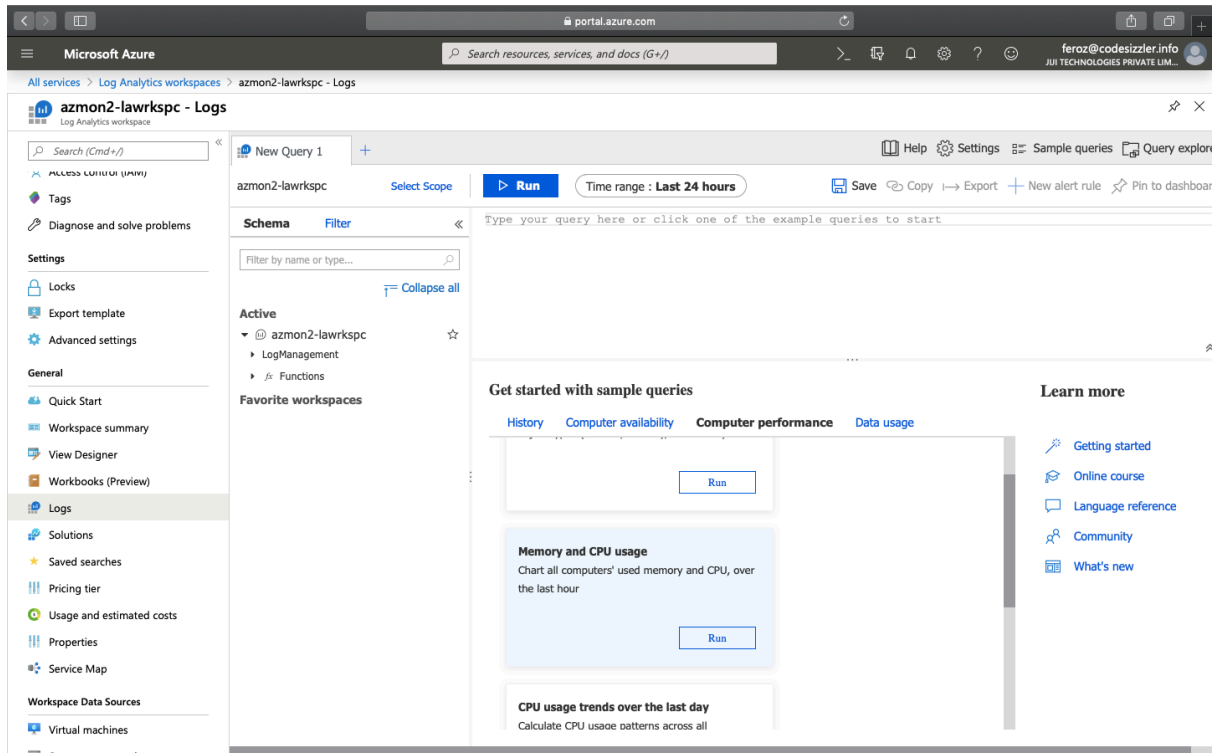
1. In the Azure portal, click **All services**, then in the search box type **Log Analytics**. As you begin typing, the list filters based on your input, and select **Log Analytics workspaces**.
2. From the list of workspaces displayed open the Log Analytics workspace we created earlier i.e. **azmon2-lawrkspc**

3. Go to **General > Performance** and select **Logs** and under **Getting started with sample queries** click on **Computer Performance** and under **Memory and CPU usage** click **Run**



4. The sample query is run, the query is displayed along with the log data output.
5. This workspace query and analysis can also be performed directly within **Azure Monitor** and the same results achieved. To do this, in the Azure Portal go to **Monitor**, and in Azure Monitor select **Logs**, and as before under **Getting started**

with sample queries click on **Computer Performance** and under **Memory and CPU usage** click **Run**.



6. The resultant query displays along with the charted output of the query for you to analyse. If you have time you can browse and run some of the other sample queries available and view the output.



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for 'feroz@codesizzler.info'. The main content area is titled 'azmon2-lawrkspc - Logs'. On the left, there is a sidebar with various navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Export template, Advanced settings), General (Quick Start, Workspace summary, View Designer, Workbooks (Preview)), Logs (selected), Solutions, Saved searches, Pricing tier, Usage and estimated costs, Properties, and Service Map. The main panel shows a 'New Query 1\*' editor. The query is a Kusto query for memory and CPU usage. The query status is 'Completed' with a duration of 00:00:01.127 and 0 records. A message states 'NO RESULTS FOUND' and '0 records matched'.

Congratulations! You have created Azure resources to provide some resources to us to monitor, then you viewed the default available monitoring data from within the virtual machine resource data, and then viewed the default available monitoring data from within Azure Monitor. You then viewed some of the monitoring options from within Azure Monitor. You then created a Log Analytics workspace, enabled Insights in your virtual machine and then reviewed the retrieved data in Azure Monitor. You then enabled diagnostic settings in the virtual machine and queried and analyzed virtual machine logs in Log Analytics workspace and Azure Monitor Logs.