

Contents

1) Create Log Analytics WorkSpace:	2
2) Configure VMInsights for the Workspace	3
3) Install Log Analytics agents on the virtual machine	8
Additional Information:	11
References :	13

1) Create Log Analytics Workspace:

Create a Log Analytics Workspace in the Central US region. Ensure that the workspace has the Log Analytics Contributor Role.

-Search for Log Analytics Workspaces and create Log Analytics workspace as below

The screenshot shows the 'Create Log Analytics workspace' page in the Azure portal. On the left, there's a sidebar with 'Log Analytics workspaces' and a search bar. The main area is titled 'Create Log Analytics workspace' and contains the following sections:

- Project details:** Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
- Subscription:** Production 1
- Resource group:** Regroup_Ogij
- Instance details:**
 - Name:** sathi-LogAnalytics
 - Region:** Central US

At the bottom, there are buttons for 'Review + Create', '< Previous', and 'Next: Pricing tier >'. Below the main form, there's a 'Pricing tier' section with a dropdown menu showing 'Pay-as-you-go (Per GB 2018)'.

Pricing tier

You can change to a Capacity Reservation tier after your workspace is created. [Learn more](#)
To learn more about access to legacy pricing tiers [click here](#)

Pricing tier *

Pay-as-you-go (Per GB 2018)

The screenshot shows the 'sathi-LogAnalytics' workspace overview page in the Azure portal. The page is titled 'sathi-LogAnalytics' and has a sidebar with navigation options like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings', 'Locks', 'Agents management', 'Agents configuration', 'Custom logs', 'Computer Groups', and 'Linked storage accounts'.

The main area is titled 'Essentials' and contains the following information:

- Resource group (change):** regroup_Ogij
- Status:** Active
- Location:** Central US
- Subscription (change):** Production 1
- Subscription ID:** f700a502-f4c5-42f4-8f1d-cacab88d7d39
- Tags (change):** [Click here to add tags](#)
- Workspace Name:** sathi-LogAnalytics
- Workspace ID:** 56302a1c-7a00-417d-ab59-40a89c0146da
- Pricing tier:** Pay-as-you-go
- Access control mode:** Use resource or workspace permissions
- Workspace state:**

Below the essentials section, there's a 'Get started with Log Analytics' section with a brief description and a list of steps:

- 1 Connect a data source
- 2 Configure monitoring solutions
- 3 Monitor workspace health

At the bottom right, there's a 'Useful links' section.

Contributor Role verification

Home > MicrosoftLogAnalyticsOMS > sathi-LogAnalytics

sathi-LogAnalytics | Access control (IAM) ...

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Agents management
Agents configuration
Custom logs
Computer Groups

+ Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access Role assignments **Roles** Roles (Classic) Deny assignments Classic administrators

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Search by role name or description Type: All Category: All

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to delete resources.	BuiltInRole	General	View
<input checked="" type="checkbox"/> Contributor	Grants full access to manage all resources, but does not allow you to delete resources.	BuiltInRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
Azure Sentinel Contributor	Azure Sentinel Contributor	BuiltInRole	Security	View
Azure Sentinel Reader	Azure Sentinel Reader	BuiltInRole	Security	View
Azure Sentinel Responder	Azure Sentinel Responder	BuiltInRole	Security	View

2) Configure VMInsights for the Workspace

Add VM Insights to the workspace created to enable all VMs to send data to Insight Metrics

Create VM1

Home >

Sathi-VM-Win1 Virtual machine

Search (Ctrl+/)

Connect Start Restart Stop Capture Delete Refresh Open in mobile

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center (previous version)
Disks
Size
Security
Advisor recommendations
Extensions

Essentials

Resource group (change): Regroup_0gij
Status: Running
Location: Central US
Subscription (change): Production 1
Subscription ID: f700a502-f4c5-42f4-8f1d-cacab88d7d39
Tags (change): [Click here to add tags](#)

Operating system: Windows
Size: Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address: 23.100.87.232
Virtual network/subnet: Regroup_0gij-vnet/default
DNS name: Not configured

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	Sathi-VM-Win1
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-Datacenter
VM generation	V1

Networking

Public IP address	23.100.87.232
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	Regroup_0gij-vnet/default
DNS name	Configure

Go to VM Insights and Enable the log analytics work space created above


Home > Sathi-VM-Win1

Sathi-VM-Win1 | Insights

Virtual machine

Search (Ctrl+/) << Resource Group Monitoring Azure Monitor Run Diagnostics Refresh Provide Feedback

- Disaster recovery
- Guest + host updates
- Inventory
- Change tracking
- Configuration management (P...
- Policies
- Run command
- Monitoring
 - Insights**
 - Alerts
 - Metrics
 - Diagnostic settings
 - Logs



Enable

The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please [click here](#).

Enable

Having difficulties enabling Azure Monitors for VM? [Troubleshoot](#)

Select log analytics created in earlier step

Resource Group Monitoring Azure Monitor Run Diagnostics Refresh Provide Feedback

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

Workspace Subscription * ⓘ

Production 1

Choose a Log Analytics Workspace ⓘ

sathi-LogAnalytics [centralus]

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.

Enable

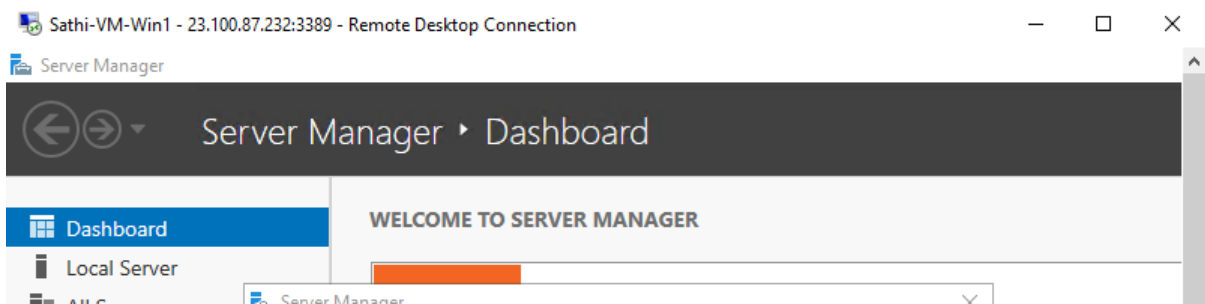
The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please [click here](#).

Enable

Insights deployment is in progress... Please wait.

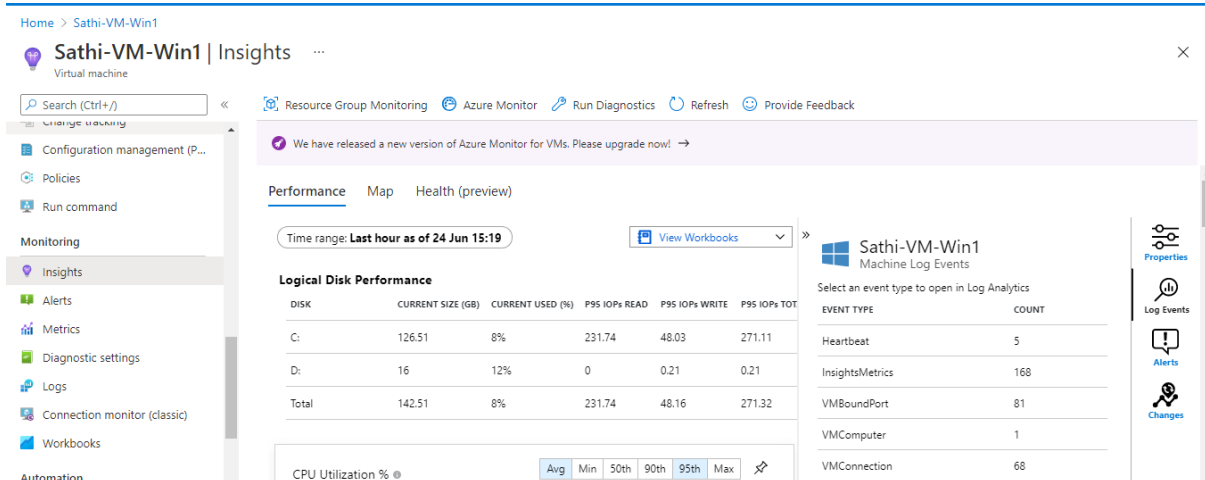
Monitoring data is being collected and routed to Insights. It can take up to 10 minutes to arrive. Please try again in a few minutes. [Workspace ID: /subscriptions/f700a502-f4c5-42f4-8f1d-cacab88d7d39/resourcegroups/regroup_0gij/providers/microsoft.operationalinsights/workspaces/sathi-loganalytics]

Login to verify VM and do some activity

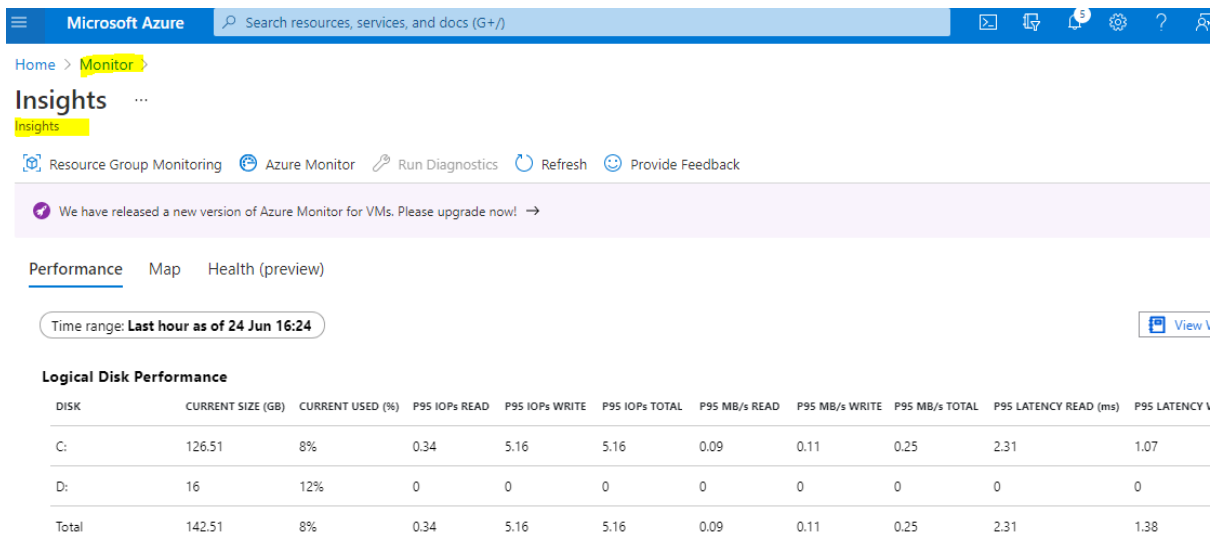


We can view all the fundamental VM insights

=> From Virtual Machine => Insights Path



=> From Monitor path : Monitor=>Virtual machines



Connect VM – LogAnalytics

-The above VM is connected to Log Analytical Workspace as we enabled in earlier step, if not navigate to Log analytics workspace data sources , click on virtual machines and select the machine to connect/disconnect

Search (Ctrl+/) << Refresh

Service Map

Workspace Data Sources

- Virtual machines
- Storage accounts logs
- System Center
- Azure Activity log
- Scope Configurations (Preview)

Name	Log Analytics Connection	OS	Subscription	Resource group	Location
Sathi-VM-Win1	✔ This workspace	Windows	f700a502-f4c5-42f4-8f1d-cac...	Regroup_0gij	centralus

When we connect VM

- LA agent (a small utility) will be installed on VM
- Inside utility, workspace id, and a key will be added - so all log info from VM will start coming to LA

Sathi-VM-Win1 ...

Virtual machine

[Connect](#) [Disconnect](#) Refresh

Status

This workspace

Workspace Name

sathi-LogAnalytics

Agent can be downloaded manually and installed on any required machine

Log Analytics workspace

Search (Ctrl+/) << Windows servers Linux servers

Tags

Diagnose and solve problems

Settings

Locks

Agents management

Agents configuration

Custom logs

Computer Groups

Linked storage accounts

Network Isolation

Advanced settings

✔ 1 Windows computers connected

[Go to logs](#)

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

[Download Windows Agent \(64 bit\)](#)[Download Windows Agent \(32 bit\)](#)

Workspace ID

56302a1c-7a00-417d-ab59-40a89c0146da

Primary key

6PvO30T5Kz5gKcyMfOsRzstSic2gCDg3pP4XrSM...

Regenerate

Secondary key

oO4r4xQvTqHBYTvLHA0B5bbwFAw55O8CUmIH...

Regenerate

Windows Events Logs Configuration :

Home > sathi-LogAnalytics

sathi-LogAnalytics | Agents configuration

Log Analytics workspace

Search (Ctrl+ /)

- Tags
- Diagnose and solve problems
- Settings
 - Locks
 - Agents management
 - Agents configuration**
 - Custom logs
 - Computer Groups
 - Linked storage accounts
 - Network Isolation
 - Advanced settings

Windows event logs Windows performance counters Linux performance counters Syslog IIS Logs

Collect Windows event log data from standard logs, like System and Application, or add custom logs created by applications you need to monitor. [Learn more](#)

+ Add windows event log

Filter event logs

Log name	Error	Warning	Information	
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Setup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Enabling Performance Counters :

sathi-LogAnalytics | Agents configuration

Log Analytics workspace

Search (Ctrl+ /)

- Tags
- Diagnose and solve problems
- Settings
 - Locks
 - Agents management
 - Agents configuration**
 - Custom logs
 - Computer Groups
 - Linked storage accounts
 - Network Isolation
 - Advanced settings

Windows event logs **Windows performance counters** Linux performance counters Syslog IIS Logs

Collect performance counters from Log Analytics agents at custom intervals to gain insight into the performance of hardware components, operating systems, and applications. [Learn more](#)
Click on the new counter name to edit it. ⓘ

+ Add performance counter

Filter performance counters

Performance counter name Sample rate (seconds)



You have no performance counter connected

Start with the recommended performance counters or use the add button to add new performance counter

Add recommended counters

Add performance counter

Query the above applied/enabled logs using KQL

The screenshot shows the Azure Log Analytics workspace interface. On the left, the 'Logs' section is selected in the sidebar. The main area displays a KQL query editor with the query 'search *'. The results table shows logs from 6/24/2021, 9:43:18.335 AM to 9:47:15.020 AM, categorized by Computer (Sathi-VM-Win1) and Type (ServiceMapCompute..., ServiceMapProcess_CL).

The screenshot shows the Azure Log Analytics workspace interface. On the left, the 'Logs' section is selected in the sidebar. The main area displays a KQL query editor with the query 'search * where Computer == "Sathi-VM-Win1" order by TimeGenerated desc'. The results table shows logs from 6/24/2021, 10:30:48.663 AM to 10:30:38.000 AM, categorized by Computer (Sathi-VM-Win1) and Source (Heartbeat, InsightsMetri...).

3) Install Log Analytics agents on the virtual machine

Install the Dependency Agent on the VM following OS-specific instructions

- **Dependency agent.** Collects discovered data about processes running on the virtual machine and external process dependencies, which are used by the [Map feature in VM insights](#). The Dependency agent relies on the Log Analytics agent to deliver its data to Azure Monitor. Deployment methods for the Dependency agent on Azure resources use the VM extension for [Windows](#) and [Linux](#).

ARM template for dependency agent *Microsoft.Azure.Monitoring.DependencyAgent deployment in VM machine -json template*

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "type": "string",
      "metadata": {
        "description": "The name of existing Azure VM. Supported Windows Server versions: 2008 R2 and above (x64)."
      }
    }
  }
}
```



```

    },
    "variables": {
      "vmExtensionsApiVersion": "2017-03-30"
    },
    "resources": [
      {
        "type": "Microsoft.Compute/virtualMachines/extensions",
        "name": "[concat(parameters('vmName'), '/DAExtension')]",
        "apiVersion": "[variables('vmExtensionsApiVersion')]",
        "location": "[resourceGroup().location]",
        "dependsOn": [
          ]
        },
        "properties": {
          "publisher": "Microsoft.Azure.Monitoring.DependencyAgent",
          "type": "DependencyAgentWindows",
          "typeHandlerVersion": "9.5",
          "autoUpgradeMinorVersion": true
        }
      }
    ],
    "outputs": {
    }
  }
}

```

Property values

Name	Value/Example
apiVersion	2015-01-01
publisher	Microsoft.Azure.Monitoring.DependencyAgent
type	DependencyAgentWindows
typeHandlerVersion	9.5

Create VM 2 , by default no extensions are deployed (vm==>Extensions)

[Home](#) > [CreateVm-MicrosoftWindowsServer.WindowsServer-201-20210624173039](#) > [Sathi-VM-Win2](#)

Sathi-VM-Win2 | Extensions

Virtual machine

<<
+ Add

Tags
 Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center (previ...
- Disks
- Size
- Security
- Advisor recommendations

Some details about the installed extensions are unavailable. This can occur when the virtual machine is stopped or the agent is unresponsive.

Name	↑↓ Type	↑↓ Version	↑↓ Status
No resource extensions found.			

Deploy the above ARM template

Custom deployment ...

Deploy from a custom template

TEMPLATE



1 resource

Edit template

Edit paramet...

Learn more

BASICS

Subscription *

Resource group *
[Create new](#)

Location

SETTINGS

Vm Name *

[Home](#) >

student_10f0devikp882u8s_00422196_vocareumvocareum.onmicrosoft.c | Overview [✈](#) ...

<< [Delete](#) [Cancel](#) [Redeploy](#) [Refresh](#)

- Overview
- Inputs
- Outputs
- Template

Your deployment is complete

Deployment name: student_10f0devikp882u8s_00422196_vocareu... Start time: 6/24/2021, 5:38:19 PM
Subscription: [Production 1](#) Correlation ID: 8898efc8-638a-4550-a5e9-50f6b3209ce7
Resource group: [Regroup_Ogij](#)

[Home](#) > [student_10f0devikp882u8s_00422196_vocareumvocareum.onmicrosoft.c](#) > [Regroup_Ogij](#) > [Sathi-VM-Win2](#)

Sathi-VM-Win2 | Extensions ...

Virtual machine

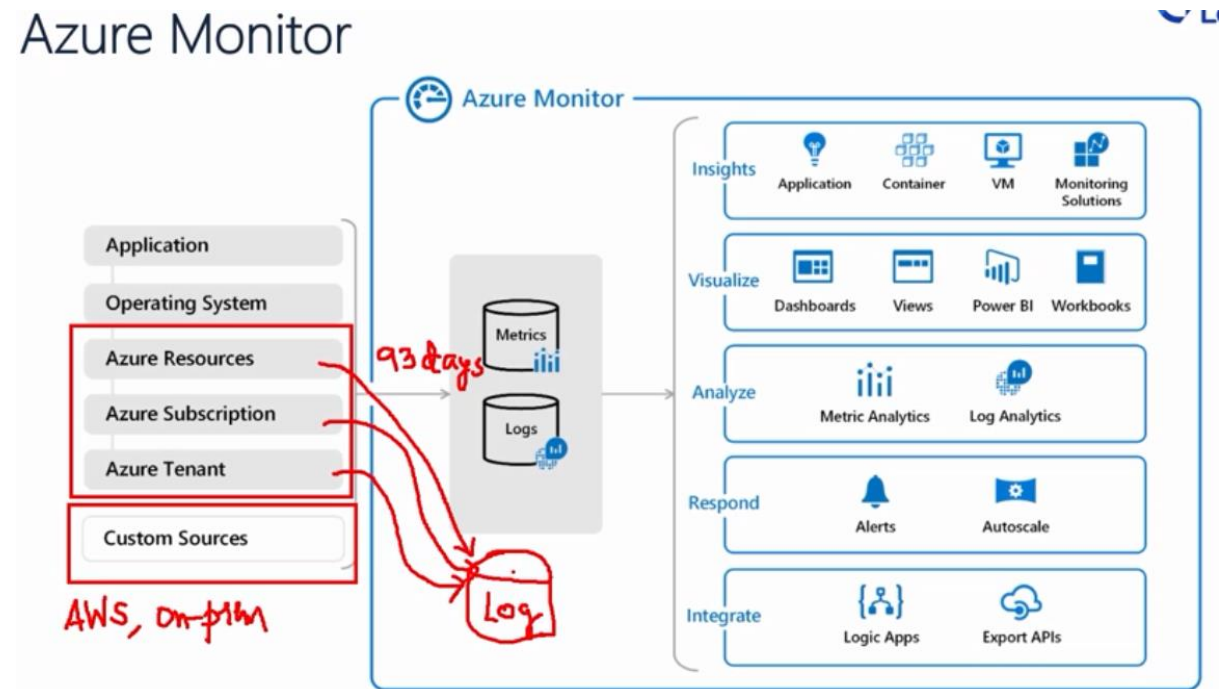
<< [+ Add](#)

- Tags
- Diagnose and solve problems
- Settings
 - Networking
 - Connect
 - Windows Admin Center (previ...
 - Disks
 - Size
 - Security

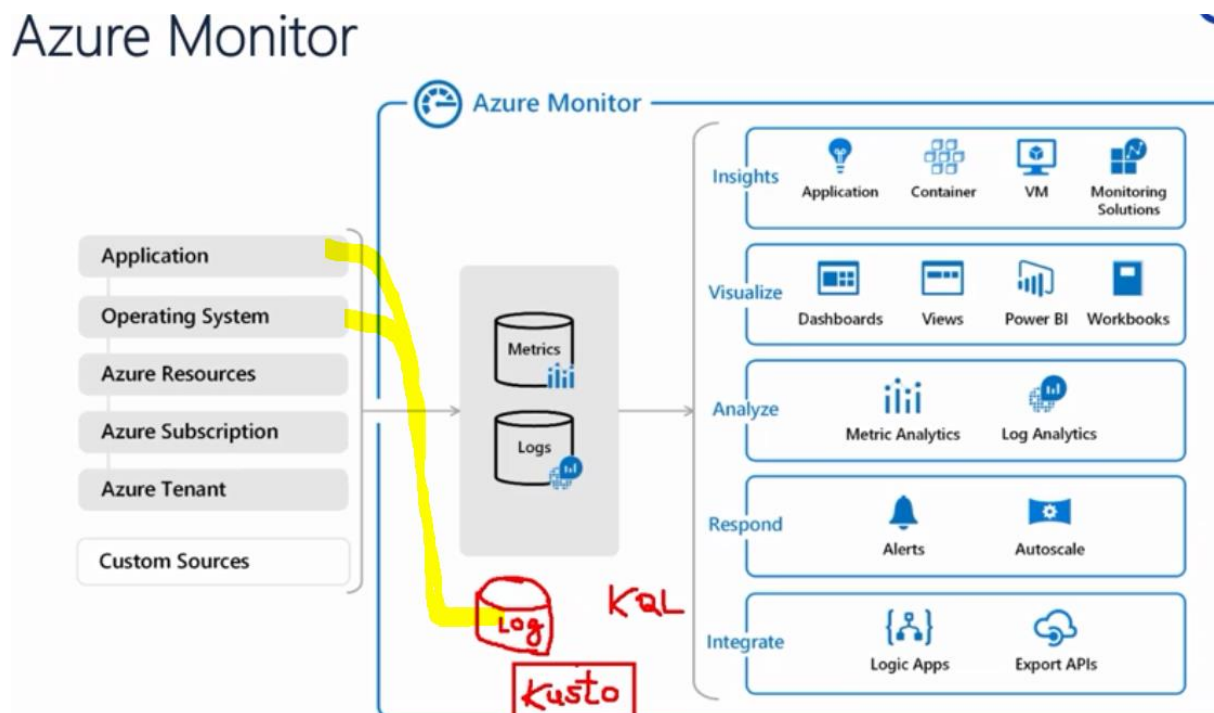
<input type="text" value="Search to filter items..."/>					
Name	↑↓	Type	↑↓	Version	↑↓
DAExtension		Microsoft.Azure.Monitoring.DependencyAgent.Dependen...		9.*	Provisioning succeeded

Assignment END

Additional Information: Azure Monitor



Azure Monitor



Activity Log

- Creation/updation/deletion of resources
- View/regenerate security keys

Metrics

- Tells us about the usage information of a resource
- Numerical numbers
- VM => CPU%, Mem%, Disk read bytes, Disk write bytes, Network in, Network out..
- Storage => Capacity used, Transactions..
- Available to us from Azure free of cost for next 93 days

Service Health

- It tells us about the health of Azure services
- 2 things
 - Current problem (Failover, inform the customers..)
 - Historical problems

Alert

- Conditions
- Action

Log Analytics

- Log db that is available from MS is called Kusto
- To query Kusto DB, you can use Kusto Query Language
- LA is a wrapper over Kusto DB
- LA wrapper allows us to capture data from various sources, setup info of what kind of data we want to capture

When we connect VM

- LA agent (a small utility) will be installed on VM
- Inside utility, workspace id, and a key will be added - so all log info from VM will start coming to LA


- Application Insights

- Capture client side logs and server side logs
- SDKs available, connectors available
- App INsights data will be stored in LA workspace



Monitor is free and available for around only 93 days history , Log Analytics needs to be used if we need to have data for more then 93 days

Home >

 **Monitor** | Overview ...

Microsoft

Search (Ctrl+/) <<

Overview

Activity log

Alerts

Metrics

Logs

Service Health

Workbooks

Insights

Applications

Virtual Machines

Storage accounts

Containers

Networks

SQL (preview)

Join us for our monthly Azure Monitor AMA - <https://aka.ms/AzMonAMABlog> →

Monitor your applications and infrastructure

Get full stack visibility, find and fix problems, optimize your performance, and understand customer behavior all in one place. [Learn more](#)



Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

[Explore Metr...](#)



Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

[Search Logs](#)



Setup Alert & Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

[Create Alert](#)

References :

<https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview>

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace>