

Final Project

Azure Log Analytics for Operations Management Suite

Problem Statement:

One of the big challenges you face with any IT Shop is to ensure a stable environment which can be only ensured if you have robust pro-active monitoring in place. The solution shouldn't non only pro-actively monitor the infrastructure but also give us analytical capabilities. Capabilities that enable us to make better use of volumes of log data

Overview of the Technology:

Azure Log Analytics is a standard service from Microsoft Azure that allows us to meet these requirements.

High Level Steps:

- 1) Install the Infrastructure to be monitored
- 2) Set up Log Analytics
- 3) Set up monitoring for the resources.
- 4) Set up Alerts using log searches
- 5) Create queries to mine important information from the log and build dashboards using them.
- 6) Perform log searches and create dashboards .

Data Source:

Azure Infrastructure

Hardware Used:

Windows 7 64 bit processor laptop

Software Used:

Python 3.6 (<https://www.python.org/downloads/>)

Azure Powershell 5.1

Log Analytics Query Language

Bash Shell

YouTube Links:

2 Min: <https://www.youtube.com/watch?v=tElv9lbLDZg&feature=youtu.be>

15 Min: <https://www.youtube.com/watch?v=Zk3SMec0Cn4> [1st part]

https://www.youtube.com/watch?v=bIOPC_rgrPI [2nd part]

GitHub:

<https://github.com/ruchitkhushu/Azure-Log-Analytics-OMS>

Contents

Creation of Initial Infrastructure	3
Creating OMS Workspace in Azure Portal:	9
Post Creation Configuration using Azure Portal	11
Creating OMS Workspace Programmatically.....	17
Adding Resources to Log Analytics Workspace through Azure Portal.....	23
Adding Resources to Log Analytics Workspace Programmatically	31
Log Search	32
OMS Portal	40
Add Solutions using OMS Portal	41
Create custom Dashboards in OMS Portal	43
Alert Management Dashboard	44
Performance dashboard for VM	45
Alerts:.....	47
Custom Alerts.....	50
Heartbeat Monitoring.....	50
Linux Service Monitoring	51
MS-SQL Server Down	53
Service Map:	55
Summary	61

Creation of Initial Infrastructure

I used a python script I have built for quickly standing up a resource group along with couple of Windows and Ubuntu VMs. Not core to this project but can be of general purpose use. I have put in my Github repository with name : **Infracreate.py**

```
C:\windows\system32\cmd.exe - python VMnet-Complex.py

C:\myPython>python UMnet-Complex.py

This script will create 2 Windows 2012 R2 VMs and 2 Ubuntu VMs along with necessary infrastructure
-----

Please enter the Subscription ID:
86d62b86-1ed2-45c1-8f6c-164c9b3db93a
-----

Please enter the resource group name:
ruchitkhushu_project_final
-----

Please enter location for your resources:
westus
-----

Please enter the name of 1st Windows 2012 R2 VM:
rk-win-vm-01
-----

Please enter the name of 2nd Windows 2012 R2 VM:
rk-win-vm-02
-----

Please enter the name of 1st Ubuntu VM:
rk-ubt-vm-01
-----

Please enter the name of 2nd Ubuntu VM:
rk-ubt-vm-02
-----

Creating resource group:ruchitkhushu_project_final.....
Resource group created. Press enter to continue...
```

```

C:\windows\system32\cmd.exe - python VMnet-Complex.py
Creating resource group:ruchitkhushu_project_final.....
Resource group created. Press enter to continue...

Creating virtual network rk_Unet.....
<'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/virtualNetworks/rk_Unet', 'nam
e': 'rk_Unet', 'type': 'Microsoft.Network/virtualNetworks', 'location': 'westus'
, 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'address_space': <a
zure.mgmt.network.v2017_03_01.models.address_space.AddressSpace object at 0x0000
0000050BDB38>, 'dhcp_options': None, 'subnets': [], 'virtual_network_peerings':
[], 'resource_guid': '0f6fed6f-9c9e-4a5b-8652-efdf22a8f7df', 'provisioning_state
': 'Succeeded', 'etag': 'W/"heb4ed66-623e-41bf-b9ed-a3aad76fbda7"'>
Press enter to continue...

Creating public IP configuration rkIPConfig01
<'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/publicIPAddresses/rkIPAddress0
1', 'name': 'rkIPAddress01', 'type': 'Microsoft.Network/publicIPAddresses', 'loc
ation': 'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'pu
blic_ip_allocation_method': 'Static', 'public_ip_address_version': 'IPv4', 'ip_c
onfiguration': None, 'dns_settings': None, 'ip_address': '138.91.245.118', 'idle
_timeout_in_minutes': 4, 'resource_guid': '93c60c2b-2c45-42f2-a4c2-072c81452c24',
'provisioning_state': 'Succeeded', 'etag': 'W/"a77c3932-d2ff-441a-9a5f-ef34cdf
7c00b"'>

Creating public IP configuration rkIPConfig02
<'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/publicIPAddresses/rkIPAddress0
2', 'name': 'rkIPAddress02', 'type': 'Microsoft.Network/publicIPAddresses', 'loc
ation': 'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'pu
blic_ip_allocation_method': 'Static', 'public_ip_address_version': 'IPv4', 'ip_c
onfiguration': None, 'dns_settings': None, 'ip_address': '138.91.241.76', 'idle
_timeout_in_minutes': 4, 'resource_guid': '359267df-098d-4a65-bbd3-bee007148695',
'provisioning_state': 'Succeeded', 'etag': 'W/"33c7c678-3bc5-4c50-bf29-965819a5
cc26"'>

Creating public IP configuration rkIPConfig03
<'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/publicIPAddresses/rkIPAddress0
3', 'name': 'rkIPAddress03', 'type': 'Microsoft.Network/publicIPAddresses', 'loc
ation': 'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'pu
blic_ip_allocation_method': 'Static', 'public_ip_address_version': 'IPv4', 'ip_c
onfiguration': None, 'dns_settings': None, 'ip_address': '138.91.252.82', 'idle
_timeout_in_minutes': 4, 'resource_guid': 'b6ba434a-74a5-4f1b-be6d-b803d5abbc76',
'provisioning_state': 'Succeeded', 'etag': 'W/"71956155-6b49-4084-8f15-818e55bd
4761"'>

Creating public IP configuration rkIPConfig04
<'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/publicIPAddresses/rkIPAddress0
4', 'name': 'rkIPAddress04', 'type': 'Microsoft.Network/publicIPAddresses', 'loc

```

```

C:\windows\system32\cmd.exe - python VMnet-Complex.py

Creating NIC rkNic04
-----
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/networkInterfaces/rkNic04', 'n
ame': 'rkNic04', 'type': 'Microsoft.Network/networkInterfaces', 'location': 'wes
tus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'virtual_machin
e': None, 'network_security_group': None, 'ip_configurations': [azure.mgmt.netw
ork.v2017_03_01.models.network_interface_ip_configuration.NetworkInterfaceIPConf
iguration object at 0x00000000053B1C88], 'dns_settings': <azure.mgmt.network.v2
017_03_01.models.network_interface_dns_settings.NetworkInterfaceDnsSettings obje
ct at 0x00000000053B1CC0>, 'mac_address': None, 'primary': None, 'enable_acceler
ated_networking': False, 'enable_ip_forwarding': False, 'resource_guid': 'cd5b7f
5e-f5bf-4dfb-945c-e0ddba57d62a', 'provisioning_state': 'Succeeded', 'etag': 'W/"
9f6ba55b-64b4-428c-b6f7-2ca82a48fc41"'>
Press enter to continue...

Creating Windows UM
-----
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-win-vm-01',
'name': 'rk-win-vm-01', 'type': 'Microsoft.Compute/virtualMachines', 'location'
: 'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'plan': N
one, 'hardware_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.
hardware_profile.HardwareProfile object at 0x00000000053A9198>, 'storage_profile'
: <azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storag
eProfile object at 0x00000000053A9828>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x00000000053A99E8>,
'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x00000000050E0C88>, 'diagnostics_profile':
None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_vie
w': None, 'license_type': None, 'vm_id': 'd8671b15-68e4-4b30-9370-b24132efeea4',
'resources': None, 'identity': None}

Creating Windows UM
-----
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-win-vm-02',
'name': 'rk-win-vm-02', 'type': 'Microsoft.Compute/virtualMachines', 'location'
: 'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'plan': N
one, 'hardware_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.
hardware_profile.HardwareProfile object at 0x00000000050C4E48>, 'storage_profile'
: <azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storag
eProfile object at 0x00000000050C4940>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x00000000050C4198>,
'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x00000000050C42E8>, 'diagnostics_profile':
None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_vie
w': None, 'license_type': None, 'vm_id': '234982c8-ea1a-4a04-ad19-13ec4d598858',
'resources': None, 'identity': None}

Press enter to continue..._

```

```

C:\windows\system32\cmd.exe - python VMnet-Complex.py

Creating Windows VM
-----
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-win-vm-02',
'name': 'rk-win-vm-02', 'type': 'Microsoft.Compute/virtualMachines', 'location':
'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'plan': N
one, 'hardware_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.
hardware_profile.HardwareProfile object at 0x00000000050C4E48>, 'storage_profile':
<azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storage
eProfile object at 0x00000000050C4940>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x00000000050C4198>,
'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x00000000050C42E8>, 'diagnostics_profile':
None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_vie
w': None, 'license_type': None, 'vm_id': '234982c8-ea1a-4a04-ad19-13ec4d598858',
'resources': None, 'identity': None}

Press enter to continue...

Creating Ubuntu VM
-----
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-ubt-vm-01',
'name': 'rk-ubt-vm-01', 'type': 'Microsoft.Compute/virtualMachines', 'location':
'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'plan': N
one, 'hardware_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.
hardware_profile.HardwareProfile object at 0x00000000053B1FD0>, 'storage_profile':
<azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storage
eProfile object at 0x00000000050EF630>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x00000000050EF588>,
'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x00000000050D00F0>, 'diagnostics_profile':
None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_vie
w': None, 'license_type': None, 'vm_id': '8ced96b2-hbed-46cd-9fba-c1ce3293f325',
'resources': None, 'identity': None}

Creating Ubuntu VM
-----
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-ubt-vm-02',
'name': 'rk-ubt-vm-02', 'type': 'Microsoft.Compute/virtualMachines', 'location':
'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'plan': N
one, 'hardware_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.
hardware_profile.HardwareProfile object at 0x00000000050C45F8>, 'storage_profile':
<azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storage
eProfile object at 0x00000000050C4898>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x00000000050C4EF0>,
'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x00000000053B1668>, 'diagnostics_profile':
None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_vie
w': None, 'license_type': None, 'vm_id': '0c9f655a-fc47-4ead-9f44-9a1100c28091',
'resources': None, 'identity': None}

Press enter to continue...

```

```

C:\windows\system32\cmd.exe
None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_view': None, 'license_type': None, 'vm_id': '8ced96b2-bbed-46cd-9fba-c1ce3293f325', 'resources': None, 'identity': None>
-----
Creating Ubuntu VM
-----
<'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-ubt-vm-02', 'name': 'rk-ubt-vm-02', 'type': 'Microsoft.Compute/virtualMachines', 'location': 'westus', 'tags': {'ccSubOwner': 'ete5f57', 'techOwner': 'eqvknmx'}, 'plan': None, 'hardware_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.hardware_profile.HardwareProfile object at 0x000000000050C45F8>, 'storage_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.StorageProfile object at 0x000000000050C4898>, 'os_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.os_profile.OSProfile object at 0x000000000050C4EF0>, 'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.network_profile.NetworkProfile object at 0x000000000053B1668>, 'diagnostics_profile': None, 'availability_set': None, 'provisioning_state': 'Succeeded', 'instance_view': None, 'license_type': None, 'vm_id': '0c9f655a-fc47-4ead-9f44-9a1100c28091', 'resources': None, 'identity': None>
-----
Press enter to continue...

Summary of the Results
-----
Resource Group Name:ruchitkhushu_project_final
Name of UM#1 is:rk-win-vm-01
Name of UM#2 is:rk-win-vm-02
Name of UM#3 is:rk-ubt-vm-01
Name of UM#4 is:rk-ubt-vm-02
-----

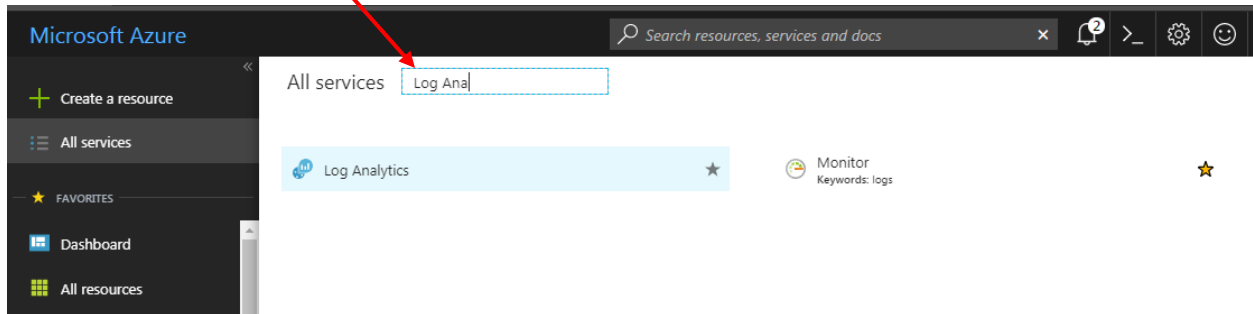
C:\myPython>_

```


Creating OMS Workspace in Azure Portal:

To start with Log Analytics we need to start with creation of OMS workspace. We can do this programmatically or using Azure portal.

Let us first see how we do it in the Portal. In the portal select All Services and then start typing “Log Analytics” in the search field



You will get the following screen listing all the workspaces for all the subscriptions and resource groups selected in the filter

Log Analytics				
McKesson Corporation				
<div> <div>+</div> Add <div>≡</div> Columns <div>↺</div> Refresh <div>🏷️</div> Assign Tags </div>				
Subscriptions: All 3 selected				
Filter by name...	All subscriptions	All resource groups	All locations	No grouping
9 items				
<input type="checkbox"/> NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION	
<input type="checkbox"/> ArkDevelopment	rg-Ark-Development	East US	Clarus - Development	...
<input type="checkbox"/> clarusmw	management-01	East US	Clarus - Development	...
<input type="checkbox"/> clarusmw-onprem	Management-01	East US	Clarus - Development	...
<input type="checkbox"/> DefaultWorkspace-35c81915-5761-4cfe-b3d2-b2b74de333f7-EUS	DefaultResourceGroup-EUS	East US	ETS SAP-HANA	...
<input type="checkbox"/> DefaultWorkspace-86d62b86-1ed2-45c1-8f6c-164c9b3db93a-EUS	DefaultResourceGroup-EUS	East US	McKesson Deep Dive Training (4)	...
<input type="checkbox"/> DefaultWorkspace-cc6b8b8a-c6f8-47b9-b10c-e61633c582ed-EUS	DefaultResourceGroup-EUS	East US	Clarus - Development	...
<input type="checkbox"/> log-analytics-92353	oms-example	West Europe	ETS SAP-HANA	...
<input type="checkbox"/> McKSAPWorkspace	SAP_Cloudera1	East US	ETS SAP-HANA	...
<input type="checkbox"/> rk-oms-wrjsp-prjf	ruchitkhushu_project_final	East US	McKesson Deep Dive Training (4)	...

Click on Add to create a new Log Analytics workspace:

Fill I the input fields in the subsequent screen to create an OMS Workspace. Below is an example. Click ok to create OMS workspace.

OMS Workspace

Create new or link existing one created in OMS ...

☒ Create New ☐ Link Existing

* OMS Workspace ⓘ

oms-test-wkspce ✓

* Subscription

McKesson Deep Dive Training (4) ▼

* Resource group ⓘ

☐ Create new ☒ Use existing

ruchitkhushu_project_final ▼

* Location

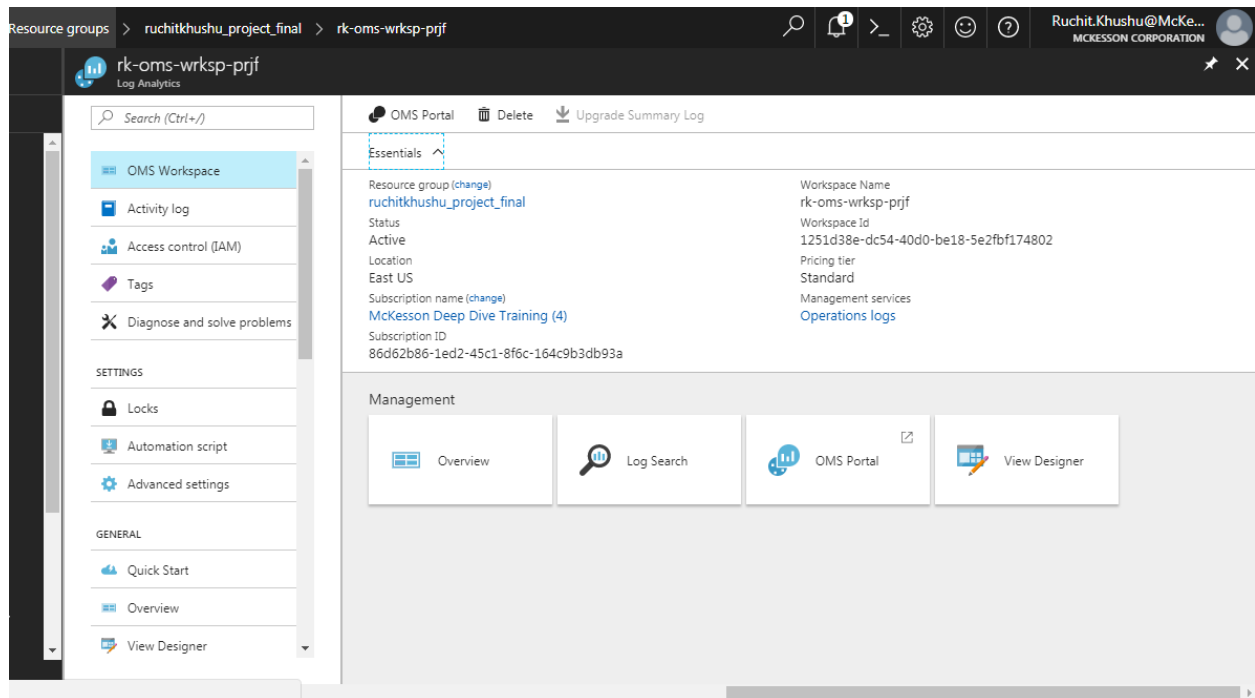
East US ▼

* Pricing tier

Free >

☐ Pin to dashboard

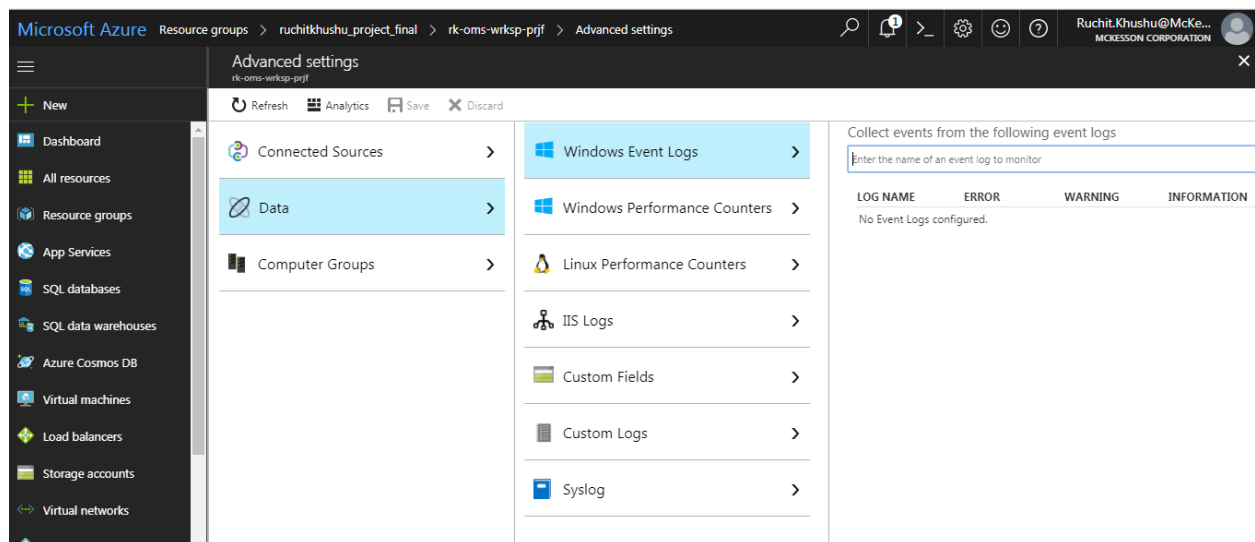
OK



Post Creation Configuration using Azure Portal

Once we have create the workspace we need to configure it . We need to define what files/data would be monitored , level of monitoring as well frequency. In this section we will see how we do it using Portal . In the section I have discuss about a PowerShell script that does it for us.

If we check the Advanced settings for OMS workspace we will see no configuration :



<div>Windows Event Logs ></div> <div>Windows Performance Counters ></div> <div>Linux Performance Counters ></div> <div>IIS Logs ></div> <div>Custom Fields ></div> <div>Custom Logs ></div> <div>Syslog ></div>	<p>Collect events from the following event logs</p> <input type="text" value="Enter the name of an event log to monitor"/> <table border="1"> <thead> <tr> <th>LOG NAME</th> <th>ERROR</th> <th>WARNING</th> <th>INFORMAT</th> </tr> </thead> <tbody> <tr> <td colspan="4">No Event Logs configured.</td> </tr> </tbody> </table>	LOG NAME	ERROR	WARNING	INFORMAT	No Event Logs configured.			
LOG NAME	ERROR	WARNING	INFORMAT						
No Event Logs configured.									

<div>Windows Event Logs ></div> <div>Windows Performance Counters ></div> <div>Linux Performance Counters ></div> <div>IIS Logs ></div> <div>Custom Fields ></div> <div>Custom Logs ></div> <div>Syslog ></div>	<p>Collect events from the following event logs</p> <input type="text" value="Enter the name of an event log to monitor"/> <table border="1"> <thead> <tr> <th>LOG NAME</th> <th>ERROR</th> <th>WARNING</th> <th>INFORMAT</th> </tr> </thead> <tbody> <tr> <td colspan="4">No Event Logs configured.</td> </tr> </tbody> </table>	LOG NAME	ERROR	WARNING	INFORMAT	No Event Logs configured.			
LOG NAME	ERROR	WARNING	INFORMAT						
No Event Logs configured.									

In order to add what Logs we want to monitor we should type the name of event log to be monitored in this field and press the + at the end of the field. We need to repeat this for every field we need.

Collect events from the following event logs

LOG NAME	ERROR	WARNING	INFORMATION
----------	-------	---------	-------------

No Event Logs configured.

Collect events from the following event logs

LOG NAME	ERROR	WARNING	INFORMATION	
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remove

Next go to Windows Performance counter:

Windows Event Logs >

Windows Performance Counters >

Linux Performance Counters >

IIS Logs >

Custom Fields >

Custom Logs >

Syslog >

Collect the following performance counters ?

Welcome!
Add some counters by searching for them in the box above, or you can
some common counters below to get started quickly.

[Add the selected performance counters](#)

- ☒ LogicalDisk(*)\Avg. Disk sec/Read
- ☒ LogicalDisk(*)\Avg. Disk sec/Write
- ☒ LogicalDisk(*)\Current Disk Queue Length
- ☒ LogicalDisk(*)\Disk Reads/sec
- ☒ LogicalDisk(*)\Disk Transfers/sec
- ☒ LogicalDisk(*)\Disk Writes/sec
- ☒ LogicalDisk(*)\Free Megabytes
- ☒ LogicalDisk(*)\% Free Space
- ☒ Memory(*)\Available MBytes
- ☒ Memory(*)\% Committed Bytes In Use
- ☒ Network Adapter(*)\Bytes Received/sec
- ☒ Network Adapter(*)\Bytes Sent/sec
- ☒ Network Interface(*)\Bytes Total/sec

Select whatever you want to monitor and click on “Add the selected performance counters”.

Advanced settings
rk-oms-wrksp-prjtf

Refresh Analytics Save Discard

Windows Event Logs

Windows Performance Counters

Linux Performance Counters

IIS Logs

Custom Fields

Collect the following performance counters ?

Enter the name of a performance counter to monitor

COUNTER NAME	SAMPLE INTERVAL
LogicalDisk(*)\% Free Space	10 seconds
LogicalDisk(*)\Avg. Disk sec/Read	10 seconds
LogicalDisk(*)\Avg. Disk sec/Write	10 seconds
LogicalDisk(*)\Current Disk Queue Length	10 seconds
LogicalDisk(*)\Disk Reads/sec	10 seconds
LogicalDisk(*)\Disk Transfers/sec	10 seconds

Next go to Linux Performance counters:

Advanced settings
rk-oms-wrksp-prjtf

Refresh Analytics Save Discard

Windows Event Logs

Windows Performance Counters

Linux Performance Counters

IIS Logs

Custom Fields

Custom Logs

Syslog

Collect the following performance counters ? ☒ Apply below configuration to my machine

Enter the name of a performance counter to monitor

Welcome!
Add some counters by searching for them in the box above, or you can add some common counters below to get started quickly.


Add the selected performance counters

- ☒ Processor(*)\% Processor Time
- ☒ Processor(*)\% Privileged Time
- ☒ Logical Disk(*)\% Used Bytes
- ☒ Logical Disk(*)\Free Megabytes
- ☒ Logical Disk(*)\% Used Space
- ☒ Logical Disk(*)\Disk Transfers/sec
- ☒ Logical Disk(*)\Disk Reads/sec
- ☒ Logical Disk(*)\Disk Writes/sec
- ☒ Memory(*)\Available MBytes Memory
- ☒ Memory(*)\% Used Memory
- ☒ Memory(*)\% Used Swap Space

Check the checkbox on right hand top corner

Collect the following performance counters ? ☒ Apply below configuration to my machine

Enter the name of a performance counter to monitor

Collect the following performance counters  ☒ Apply below configuration to my machine





Enter the name of a performance counter to monitor

COUNTER NAME	INSTANCE	SAMPLE INTERVAL	
Logical Disk	<input type="text" value="*"/>	<input type="text" value="10"/> seconds	
% Used Inodes			Remove
Free Megabytes			Remove
% Used Space			Remove
Disk Transfers/sec			Remove
Disk Reads/sec			Remove
Disk Writes/sec			Remove
Memory	<input type="text" value="*"/>	<input type="text" value="10"/> seconds	
Available MBytes Memory			Remove
% Used Memory			Remove
% Used Swap Space			Remove
Network	<input type="text" value="*"/>	<input type="text" value="10"/> seconds	
Total Bytes Transmitted			Remove
Total Bytes Received			Remove


In the screen above you can make changes or go with default values. Next Save the settings

Advanced settings

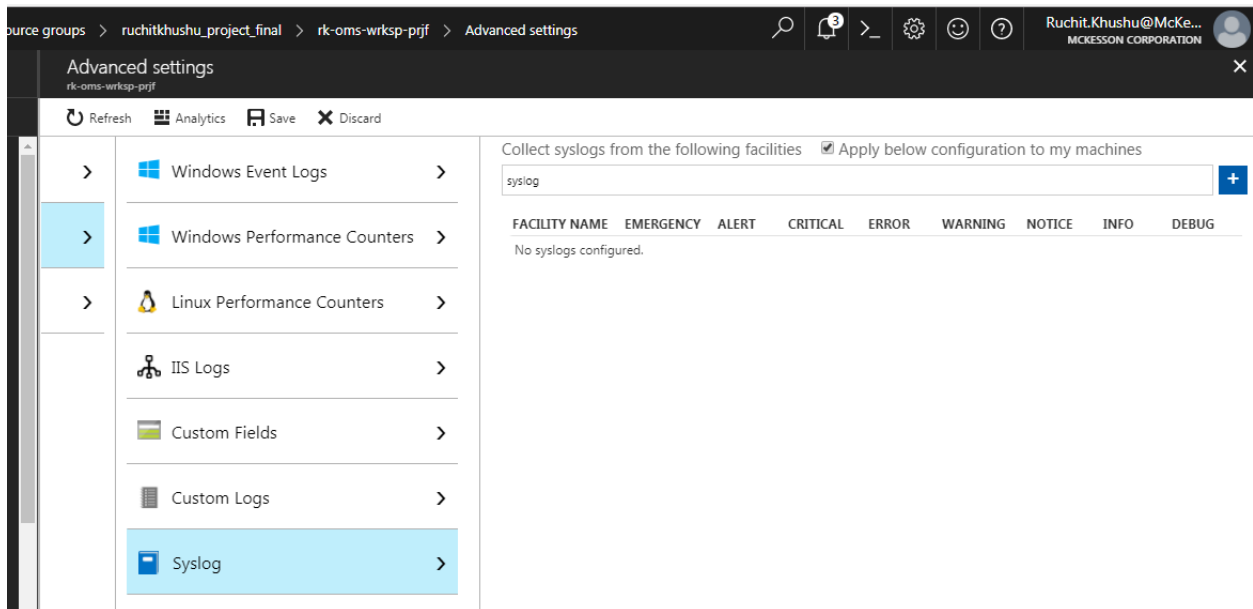
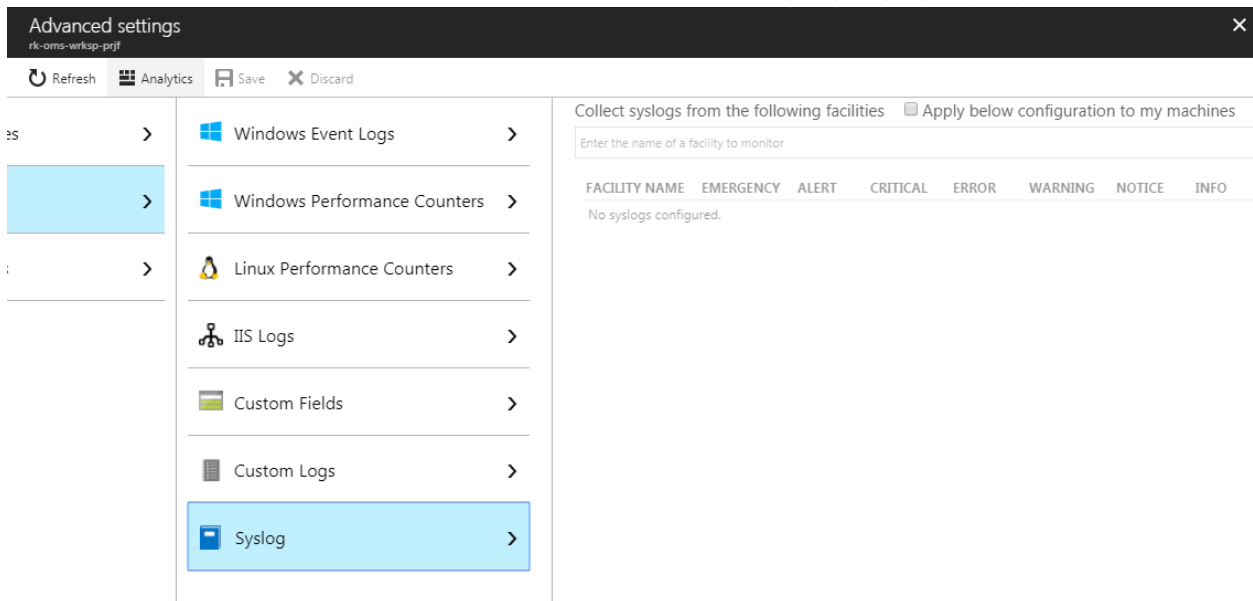
rk-oms-wrksp-prj

 Refresh
  Analytics
  Save
  Discard

Configuration was successfully saved.

OK 

Next I configured SYSLOG:



Collect syslogs from the following facilities ☒ Apply below configuration to my machines

syslog +

FACILITY NAME	EMERGENCY	ALERT	CRITICAL	ERROR	WARNING	NOTICE	INFO	DEBUG
No syslogs configured.								

I added syslog and kern facilities.. For syslog type “syslog” in the field and then click on blue “+” button

Collect syslogs from the following facilities ☒ Apply below configuration to my machines

Enter the name of a facility to monitor +

FACILITY NAME	EMERGENCY	ALERT	CRITICAL	ERROR	WARNING	NOTICE	INFO	DEBUG	
kern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remove
syslog	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Remove

Finally save the settings.

Advanced settings
rk-oms-wrksp-prj

Refresh
 Analytics
 Save
 Discard

Creating OMS Workspace Programmatically

This is how we create Log Analytics Workspace Programmatically . Basically the cmdlet **New-AzureRMOperationalInsightsWorkspace** is used for this:

Administrator: Windows PowerShell ISE

```

1 Select-AzureRmSubscription -Subscription 'McKesson Deep Dive Training (4)'
2 $ResourceGroup='ruchitkhushu_project_final'
3 $WorkspaceName='rk-oms-wrksp-prjtf'
4 $Location='eastus'
5 New-AzureRmOperationalInsightsWorkspace -Location $Location -Name $WorkspaceName -Sku Standard -ResourceGroupName $ResourceGroup
6

```

```

Name                : [Ruchit.Khushu@McKesson.com, 86d62b86-1ed2-45c1-8f6c-164c9b3db93a]
Account             : Ruchit.Khushu@McKesson.com
SubscriptionName     : McKesson Deep Dive Training (4)
TenantId            : da67ef1b-ca59-4db2-9a8c-aa8d94617a16
Environment         : AzureCloud

Name                : rk-oms-wrksp-prjtf
ResourceId          : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourcegroups/ruchitkhushu_project_final/providers/microsoft.operational
ResourceGroupName   : ruchitkhushu_project_final
Location            : eastus
Tags                : [[ccSubOwner, etesf37], [techOwner, eqvknmx]]
Sku                 : standard
RetentionInDays     : 30
CustomerId          : 1251d38e-dc54-40d0-be18-5e2fbf174802
PortalUrl           : https://eus.mms.microsoft.com/Account?tenant=da67ef1b-ca59-4db2-9a8c-aa8d94617a16&resource=2fsubscriptions%2f86d62b86-1ed2-4
                    5c1-8f6c-164c9b3db93a%2fresourcegroups%2fruchitkhushu_project_final%2fproviders%2fmicrosoft.operationalinsights%2fworkspaces%
                    2frk-oms-wrksp-prjtf
ProvisioningState    : Succeeded

```

Completed

Ln 1 Col 1 100%

However the above screenshot is a very simply script just creating a workspace. I created a PowerShell script which asks user for input like Resource group name + Workspace name and then goes on to create the workspace and do the configuration work for us. Of course the configuration is purely what has been defined in the script.. Anyone can omit or add monitors in the config part of the script.

```

Administrator: Windows PowerShell

PS D:\Scripts\bin> .\NEWOMS.ps1
Input the subscription ID:: 86d62b86-1ed2-45c1-8f6c-164c9b3db93a

Account      : Ruchit.Khushu@McKesson.com
SubscriptionName : McKesson Deep Dive Training (4)
SubscriptionId  : 86d62b86-1ed2-45c1-8f6c-164c9b3db93a
TenantId       : da67ef1b-ca59-4db2-9a8c-aa8d94617a16
Environment    : AzureCloud

Input your resource group name: ruchitkhushu_prj_finale
Input your workspace name: wrkspacoms
Checking if resource group exists. If not will create the resource group

ResourceGroupName : ruchitkhushu_prj_finale
Location           : eastus
ProvisioningState   : Succeeded
Tags               :
TagsTable          :
ResourceId          : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale

Creating the workspace
Name           : wrkspacoms
ResourceId      : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
s/microsoft.operationalinsights/workspaces/wrkspacoms
ResourceGroupName : ruchitkhushu_prj_finale
Location         : eastus
Tags             : [{"ccSubOwner", "ete5f57"}, {"techOwner", "eqvknmx"}]
Sku              : standard
RetentionInDays   : 30
CustomerId        : ab385f3f-7626-4035-81fc-84b3635b9e72
PortalUrl         : https://eus.mms.microsoft.com/Account?tenant=da67ef1b-ca59-4db2-9a8c-aa8d94617a16&resource=%2fsubscriptions%2f86d62b86-1ed2-45c1-8f6c-164c9b3db93a%2fresourceGroups%2fruchitkhushu_prj_finale%2fproviders%2fmiicrosoft.operationalinsights%2fworkspaces%2fwrkspacoms
ProvisioningState : Succeeded

Setting up Windows Event Monitors

Name           : Example Application Event Log
ResourceId      : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
s/Microsoft.OperationalInsights/workspaces/wrkspacoms/datasources/Example Application Event Log
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName     : wrkspacoms
Kind              : WindowsEvent
Properties         : {"eventLogName": "Application", "eventTypes": [{"eventType": "Error"}, {"eventType": "Warning"}]}

Name           : System Event Log
ResourceId      : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
s/Microsoft.OperationalInsights/workspaces/wrkspacoms/datasources/System Event Log
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName     : wrkspacoms
Kind              : WindowsEvent
Properties         : {"eventLogName": "System", "eventTypes": [{"eventType": "Error"}, {"eventType": "Warning"}]}

Setting up Windows Performance Monitors

```

```

Administrator: Windows PowerShell

Properties      : {"state":"Enabled"}
Setting up Linux Syslog Monitors
Name           : Linux syslog collection
ResourceId     : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
               : s/Microsoft.OperationalInsights/workspaces/wrkspaceoms/datasources/Linux syslog collection
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName    : wrkspaceoms
Kind            : LinuxSyslog
Properties       : {"syslogName":"syslog","syslogSeverities":[{"severity":"emerg"}, {"severity":"alert"}, {"severity":"crit"}, {"severity":"err"}, {"severity":"warning"}]}

Name           : Linux Kernal collection
ResourceId     : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
               : s/Microsoft.OperationalInsights/workspaces/wrkspaceoms/datasources/Linux Kernal collection
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName    : wrkspaceoms
Kind            : LinuxSyslog
Properties       : {"syslogName":"kern","syslogSeverities":[{"severity":"emerg"}, {"severity":"alert"}, {"severity":"crit"}, {"severity":"err"}, {"severity":"warning"}]}

Name           : DataSource_LinuxSyslogCollection
ResourceId     : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
               : s/Microsoft.OperationalInsights/workspaces/wrkspaceoms/datasources/DataSource_LinuxSyslogCollection
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName    : wrkspaceoms
Kind            : LinuxSyslogCollection
Properties       : {"state":"Enabled"}

Setting up IIS Log collection
Name           : DataSource_IISLogs
ResourceId     : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchitkhushu_prj_finale/provider
               : s/Microsoft.OperationalInsights/workspaces/wrkspaceoms/datasources/DataSource_IISLogs
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName    : wrkspaceoms
Kind            : IISLogs
Properties       : {"state":"OnPremiseEnabled"}

List enabled solution
Name           : LogManagement
Enabled        : True

This script allows you to additional set up following solutions:
Alert Monitoring
Do you want to enable the solution Alert Management ? Answer in Y or N only: y

Name           : AlertManagement
Enabled        : True

PS D:\Scripts\bin>

```

The powershell script is : [I will also put it on Github with name : **OMSconfig.ps1**]

```

$subscriptionid=Read-Host 'Input the subscription ID:'
Login-AzureRmAccount -subscriptionid $subscriptionid
$ResourceGroup = Read-Host -Prompt 'Input your resource group name'
$WorkspaceName = Read-Host -Prompt 'Input your workspace name'
$Location = "eastus"

write-host 'checking if resource group exists. If not will create the resource group'

# Create the resource group if needed
try {
    Get-AzureRmResourceGroup -Name $ResourceGroup -ErrorAction Stop
} catch {
    New-AzureRmResourceGroup -Name $ResourceGroup -Location $Location
}

```

```

write-host 'Creating the workspace'

# Create the workspace
New-AzureRmOperationalInsightsworkspace -Location $Location -Name $WorkspaceName -Sku
Standard -ResourceGroupName $ResourceGroup

write-host 'Setting up Windows Event Monitors'

# Windows Event Configuration

New-AzureRmOperationalInsightsWindowsEventDataSource -ResourceGroupName $ResourceGroup
-WorkspaceName $WorkspaceName -EventLogName "Application" -CollectErrors -
CollectWarnings -Name "Example Application Event Log"

New-AzureRmOperationalInsightsWindowsEventDataSource -ResourceGroupName $ResourceGroup
-WorkspaceName $WorkspaceName -EventLogName "System" -CollectErrors -CollectWarnings -
Name "System Event Log"

write-host 'Setting up Windows Performance Monitors'

# Windows Performance Configuration

write-host 'Setting up Windows Performance Monitors'

New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Logical Disk" -InstanceName
"*" -CounterName ("% Free Space") -IntervalSeconds 10 -Name " windows Logical Disk
Performance Counter-1"
New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Logical Disk" -InstanceName
"*" -CounterName ("Avg. Disk sec/Read") -IntervalSeconds 10 -Name " windows Logical
Disk Performance Counter-2"
New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Logical Disk" -InstanceName
"*" -CounterName ("Avg. Disk sec/Write") -IntervalSeconds 10 -Name " windows Logical
Disk Performance Counter-3"
New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Logical Disk" -InstanceName
"*" -CounterName ("Current Disk Queue Length") -IntervalSeconds 10 -Name " windows
Logical Disk Performance Counter-4"

New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Memory" -InstanceName "*" -
CounterName ("% Committed Bytes In Use") -IntervalSeconds 10 -Name " windows Memory
Performance Counter-1"
New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Memory" -InstanceName "*" -
CounterName ("Available MBytes") -IntervalSeconds 10 -Name " windows Performance
Counter-2"

New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Network Adapter" -
InstanceName "*" -CounterName ("Bytes Received/sec ") -IntervalSeconds 20 -Name
"Windows Network Adapter Performance Counter-1"
New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Network Adapter" -
InstanceName "*" -CounterName ("Available MBytes") -IntervalSeconds 20 -Name " windows
Network Adapter Performance Counter-2"

New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Network Interface" -
InstanceName "*" -CounterName ("Bytes Total/sec") -IntervalSeconds 20 -Name "Windows
Network Interface Performance Counter-1"

New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Processor" -InstanceName "*"
-CounterName ("% Processor Time") -IntervalSeconds 10 -Name "Windows Processor
Performance Counter-1"

```

```
New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "System" -InstanceName "*" -
CounterName ("Processor Queue Length") -IntervalSeconds 10 -Name "Windows System
Performance Counter-1"
```

```
# Setting Up Linux Performance Counters
```

```
write-host 'Setting up Linux Performance Monitors'
```

```
New-AzureRmOperationalInsightsLinuxPerformanceObjectDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Network" -InstanceName "*"
-CounterNames @("%Processor Time", "%Privileged Time") -IntervalSeconds 20 -Name
"Linux Processor Performance Counters"
```

```
New-AzureRmOperationalInsightsLinuxPerformanceObjectDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Logical Disk" -InstanceName
"*" -CounterNames @("% Used Inodes", "Free Megabytes", "% Used Space", "Disk
Transfers/sec", "Disk Reads/sec", "Disk Reads/sec", "Disk Writes/sec") -
IntervalSeconds 10 -Name "Linux Disk Performance Counters "
```

```
New-AzureRmOperationalInsightsLinuxPerformanceObjectDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Memory" -InstanceName "*" -
CounterNames @("Available Mbytes Memory", "%User Memory", "% Used Swap Space") -
IntervalSeconds 10 -Name "Linux Memory Performance Counters"
Enable-AzureRmOperationalInsightsLinuxPerformanceCollection -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName
```

```
# Linux Syslog
```

```
write-host 'Setting up Linux Syslog Monitors'
```

```
New-AzureRmOperationalInsightsLinuxSyslogDataSource -ResourceGroupName $ResourceGroup
-WorkspaceName $WorkspaceName -Facility "syslog" -CollectEmergency -CollectAlert -
CollectCritical -CollectError -CollectWarning -Name "Linux syslog collection"
```

```
New-AzureRmOperationalInsightsLinuxSyslogDataSource -ResourceGroupName $ResourceGroup
-WorkspaceName $WorkspaceName -Facility "kern" -CollectEmergency -CollectAlert -
CollectCritical -CollectError -CollectWarning -Name "Linux kernal collection"
```

```
Enable-AzureRmOperationalInsightsLinuxSyslogCollection -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName
```

```
# Enable IIS Log Collection using agent
```

```
write-host 'Setting up IIS Log collection'
```

```
Enable-AzureRmOperationalInsightsIISLogCollection -ResourceGroupName $ResourceGroup -
WorkspaceName $WorkspaceName
```

```
#List enabled solutions
```

```
write-host 'List enabled solution'
(Get-AzureRmOperationalInsightsIntelligencePacks -ResourceGroupName $ResourceGroup -
WorkspaceName $WorkspaceName).where({($_.enabled -eq $true)})
```

```
write-host 'This script allows you to additional set up following solutions:'
write-host 'Alert Monitoring'
$userdec = read-host 'Do you want to enable the solution Alert Management ? Answer in
Y or N only'
```

```
if ($userdec="Y")
{
    Set-AzureRmOperationalInsightsIntelligencePack -ResourceGroupName $ResourceGroup -
workspaceName $WorkspaceName -IntelligencePackName 'AlertManagement' -Enabled $true
}
```

Adding Resources to Log Analytics Workspace through Azure Portal





Immediately after the OMS workspace is created nothing is added to the Workspace. You can check under Advanced Settings → Connected Systems:


We can add following sources to OMS workspace:


1. Azure VMs (also storage accounts)
2. On -Premise systems


For this project we have used Azure resources only.


In order to do so please go to section Workspace Data Sources inside the Log Analytics workspace we have created.

 Windows Servers >	Windows Servers Attach any Windows server or client.
 Linux Servers >	0 WINDOWS COMPUTERS CONNECTED
 Azure Storage >	Download Windows Agent (64 bit)
 System Center >	Download Windows Agent (32 bit)
	You'll need the Workspace ID and Key to install the agent.
	WORKSPACE ID
	1251d38e-dc54-40d0-be18-5e2fbf174802
	PRIMARY KEY
	RyLEbIpXZQVFHgPsPs41KpV6jVBkoDqXcgr

 Windows Servers >

 Linux Servers >

 Azure Storage >

 System Center >

Linux Servers

Attach any Linux server or client.

0 LINUX COMPUTERS CONNECTED

[Download Agent for Linux](#)

You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID

1251d38e-dc54-40d0-be18-5e2fbf174802

PRIMARY KEY


RyLEb1pXZQVFHgPsPs41KpV6jVBkoDqXcgf


[Regenerate](#)


SECONDARY KEY


z2IocvY1wJ/TAU8CEDQh8LU6tvRVfZL/p19X

[Regenerate](#)

 Windows Servers >

 Linux Servers >

 Azure Storage >





 System Center >

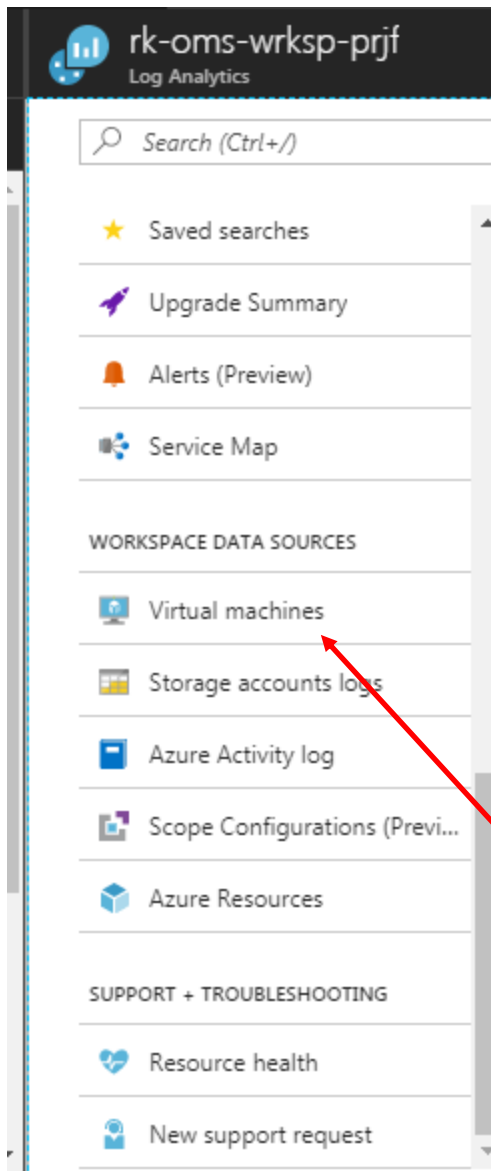
Azure Storage Account

Attach any Azure storage account configured with the Windows or Linux Azure Diagnostic VM extension.

0 STORAGE ACCOUNTS CONNECTED



























[View Documentation](#)

<div> Windows Servers ></div>	<div>System Center Operations Manager</div> <div>Attach your management groups or your entire Operations Manager deployment with just a few clicks.</div> <div>View Documentation</div> <div>0 MGMT GROUPS CONNECTED</div>
<div> Linux Servers ></div>	
<div> Azure Storage ></div>	
<div> System Center ></div>	



Let us add virtual machines to it. Inside the workspace click on virtual machines

Refresh ? Help

Filter by name...	8 selected	2 selected	3 selected	47 selected	5 selected
NAME	OMS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
 ad-primary-dc	 Other workspace	Windows	35c81915-5761-4cfe-b3...	ALWAYSONTEST01	westus
 ad-primary-dc	 Other workspace	Windows	35c81915-5761-4cfe-b3...	SQLALWAYSONTEST01	westus
 ad-secondary-dc	 Other workspace	Windows	35c81915-5761-4cfe-b3...	SQLALWAYSONTEST01	westus
 ad-secondary-dc	 Other workspace	Windows	35c81915-5761-4cfe-b3...	ALWAYSONTEST01	westus
 aks-nodepool1-378741...	 Not connected	Linux	86d62b86-1ed2-45c1-8f...	MC_shaqrg-shaqrgAKS...	eastus
 aks-nodepool1-378741...	 Not connected	Linux	86d62b86-1ed2-45c1-8f...	MC_shaqrg-shaqrgAKS...	eastus
 AnsiblePOC	 Not connected	Linux	35c81915-5761-4cfe-b3...	RG-VNET-ETSHANA	westus
 cluster-fsw	 Other workspace	Windows	35c81915-5761-4cfe-b3...	SQLALWAYSONTEST01	westus
 cluster-fsw	 Other workspace	Windows	35c81915-5761-4cfe-b3...	ALWAYSONTEST01	westus
 csrvpn1	 Not connected	Linux	cc6b8b8a-c6f8-47b9-b1...	RG-ETSNETWORK	eastus2
 DOFHSLES12	 Error	Linux	35c81915-5761-4cfe-b3...	SAP_CLOUDERA1	westus
 e2p-alt-ctl-01	 Other workspace	Windows	cc6b8b8a-c6f8-47b9-b1...	PRODUCTION	eastus
 e2p-alt-ctl-01	 Other workspace	Windows	cc6b8b8a-c6f8-47b9-b1...	PRODUCTION	eastus

You need to select the VM you want to add to the workspace. Please note 1 VM can be added to 1 Workspace at any given point of time.. We can manually filter by Virtual machine name or broader criteria like Subscription name, Resource group name etc.

Refresh

Help

Filter by name...









8 selected

2 selected

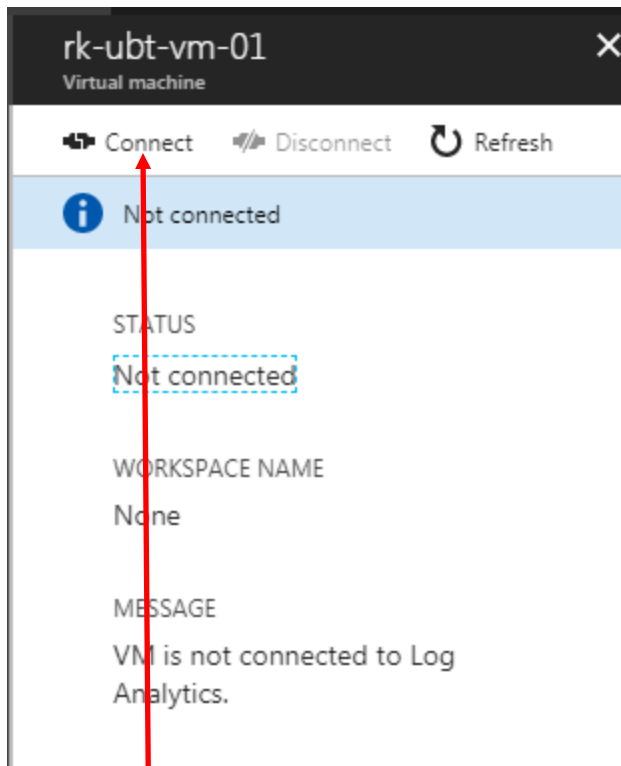
McKesson Deep Div...

ruchitkhushu_projec...

5 selected

NAME	OMS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
 rk-ubt-vm-01	 Not connected	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-ubt-vm-02	 Not connected	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-win-vm-01	 Not connected	Windows	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-win-vm-02	 Not connected	Windows	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus

Click on the VM and connect to OMS



Select "Connect"

rk-ubt-vm-01

Virtual machine

Connect

Disconnect

Refresh

Connecting...

STATUS

Connecting

WORKSPACE NAME

rk-oms-wrksp-prjf

MESSAGE

Connecting VM to Log Analytics.
Please check back later for status
update.

rk-ubt-vm-01

Virtual machine

Connect

Disconnect

Refresh









STATUS

This workspace









WORKSPACE NAME

rk-oms-wrksp-prjf

MESSAGE

Refresh ? Help					
Filter by name... 8 selected 2 selected McKesson Deep Div... ruchitkhushu_projec... 5 selected					
NAME	OMS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
 rk-ubt-vm-01	 This workspace	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-ubt-vm-02	 Not connected	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-win-vm-01	 Not connected	Windows	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-win-vm-02	 Not connected	Windows	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus

Do it for all the VMs that need to be connected...

Refresh ? Help					
Filter by name... 8 selected 2 selected McKesson Deep Div... ruchitkhushu_projec... 5 selected					
NAME	OMS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
 rk-ubt-vm-01	 This workspace	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-ubt-vm-02	 This workspace	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-win-vm-01	 This workspace	Windows	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
 rk-win-vm-02	 This workspace	Windows	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus

If we now go to Advanced settings and to Connected systems:

Advanced settings
rk-oms-wrksp-prj

Connected Sources >

Windows Servers >

Windows Servers

Attach any Windows server or client.

2 WINDOWS COMPUTERS CONNECTED

Advanced settings
rk-oms-wrksp-prj

Connected Sources >

Windows Servers >

Linux Servers >

Linux Servers

Attach any Linux server or client.

2 LINUX COMPUTERS CONNECTED

Download Agent for Linux

Adding Resources to Log Analytics Workspace Programmatically

Adding VM one by one to Azure Portal can be cumbersome if there are too many VMs. So we can do it programmatically using PowerShell

I have created a simple script that adds Virtual Machines to OMS workspace. The program takes a .csv file as input. The .csv file has VMName, Resource Group and Location columns. Below is the code. I will add it to Github with the name :**OMSAddResource.ps1**

```
$subscriptionid=Read-Host 'Input the subscription ID:'
Login-AzureRmAccount -subscriptionid $subscriptionid

$FILE = Read-Host -Prompt 'Input the full path along with the file name with VM Name
and Resource Group Information'
$omsId = Read-Host -Prompt 'Input your OMS workspace ID'

$omsKey = Read-Host -Prompt 'Input your OMS workspace Key'
Write-Host 'Installing and Configing the OMS Key.'

Import-CSV $file | ForEach-Object {

    $vmName = $_.VMName
    $resourceGroup = $_.ResourceGroup
    $location = $_.Location

    Write-Host "Installing and Configing the OMS Key for $vmName."

    # Install and configure the OMS agent
    try {

        $PublicSettings = New-Object psobject | Add-Member -PassThru NoteProperty workspaceId
        $omsId | ConvertTo-Json
        $protectedSettings = New-Object psobject | Add-Member -PassThru NoteProperty
        workspaceKey $omsKey | ConvertTo-Json

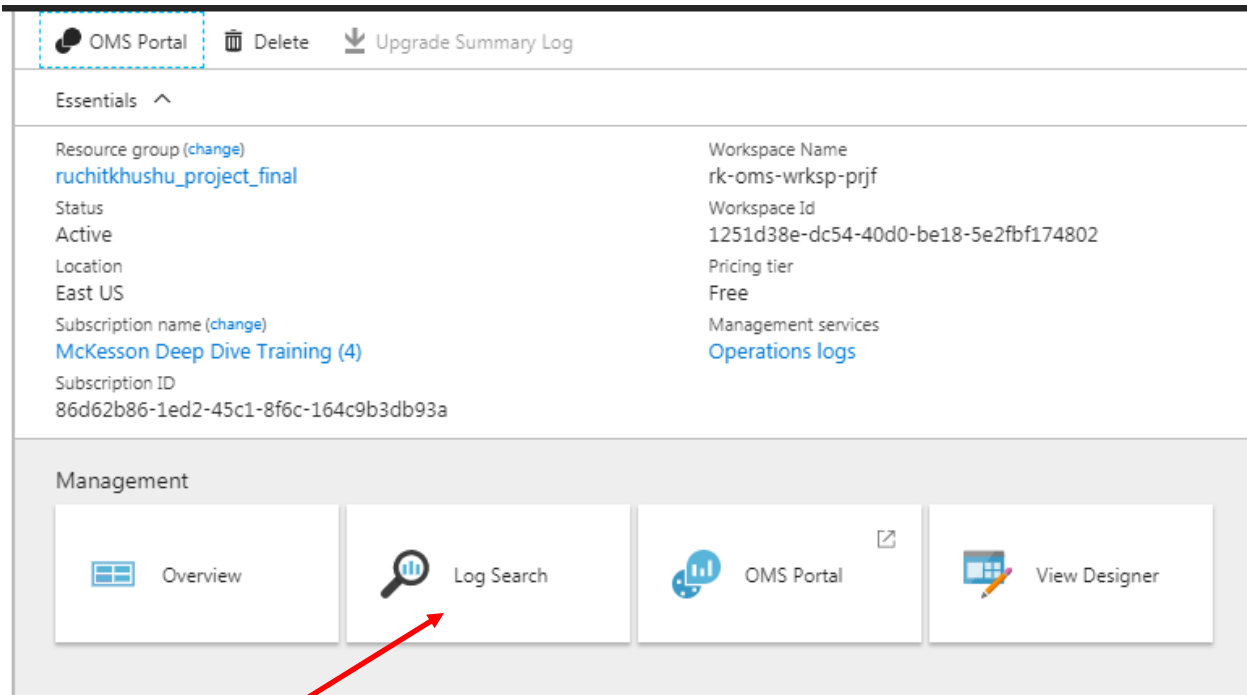
        Set-AzureRmVMExtension -ExtensionName "OMS" -ResourceGroupName $resourceGroup -VMName
        $vmName
        -Publisher "Microsoft.EnterpriseCloud.Monitoring" -ExtensionType
        "MicrosoftMonitoringAgent"
        -TypeHandlerVersion 1.0 -SettingString $PublicSettings ` -ProtectedSettingString
        $protectedSettings -Location $location
        write-host "Setup OMS for VM: $vmname in resource group: $resourceGroup successful" -
        ErrorAction Stop
    } catch {

        write-host "Setup OMS for VM: $vmname in resource group: $resourceGroup failed"
    }

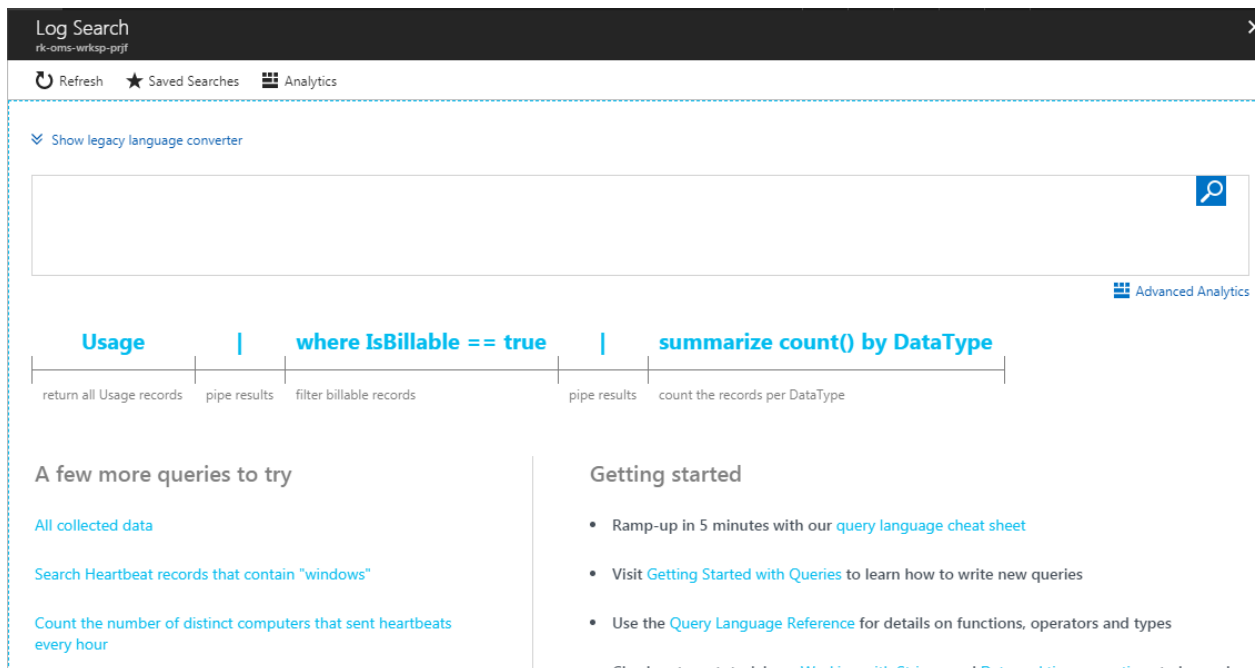
}
```

Log Search

Now that our Log Analytics set up is done and data has started flowing in we can perform Log search using Log query



Click on Log search



Log Search
rk-oms-wrksp-prjtf

Refresh
Saved Searches
Analytics

Show legacy language converter

Perf

Perf |

Usage

where IsBillable == true

summarize count() by DataType

return all Usage records
pipe results
filter billable records
pipe results
count the records per DataType

In the field above we can type our queries . Let us type Perf and check the output

Log Search
rk-oms-wrksp-prjtf

Refresh
Saved Searches
Analytics
New Alert Rule
Export
PowerBI

Data based on last 1 day
1 bar = 1hr

TYPE (1)
Perf
3M

OBJECTNAME (8)
LogicalDisk 954K
Network Adapter 874K
Logical Disk 516K
+Add

Show legacy language converter
Perf
Advanced Analytics
00:00:00

3M Results
List
Table
2/16/2018 12:28:39.680 PM | Perf
Computer : rk-ubt-vm-01
ObjectName : Logical Disk
CounterName : Free Megabytes
InstanceName : /
CounterValue : 26590
TimeGenerated : 2/16/2018 12:28:39.680 PM
CounterPath : \\rk-ubt-vm-01\Logical Disk(\)\Free Megabytes
Computer_CF : 01
[+] show more

You can see there are 3 Million records.. On the left side you see various dimensions of these records like OBJECTNAME,COUNTERNAME, COMPUTER etc.

OBJECTNAME (8)		×
<input type="checkbox"/>	LogicalDisk	954K
<input type="checkbox"/>	Network Adapter	874K
<input type="checkbox"/>	Logical Disk	516K
<input type="checkbox"/>	Processor	160K
<input type="checkbox"/>	Memory	157K

[+] More

COUNTERNAME (23)		×
<input type="checkbox"/>	Bytes Received/sec	437K
<input type="checkbox"/>	Bytes Sent/sec	437K
<input type="checkbox"/>	Disk Writes/sec	205K
<input type="checkbox"/>	Free Megabytes	205K
<input type="checkbox"/>	Disk Transfers/sec	205K

+Add

COMPUTER_CF (5) ×	
<input type="checkbox"/> 01	981K
<input type="checkbox"/> 02	973K
<input type="checkbox"/> 00	302K
<input type="checkbox"/>	292K
<input type="checkbox"/> 03	284K

COMPUTER (9) ×	
<input type="checkbox"/> rk-win-vm-01	448K
<input type="checkbox"/> rk-win-vm-02	448K
<input type="checkbox"/> rk-vm-00	302K
<input type="checkbox"/> rk-cent-vm-01	301K
<input type="checkbox"/> rk-vm-02	293K

[+] More

+Add

We can add filters to this query by selecting the dimensions

COMPUTER (9) ×	
<input checked="" type="checkbox"/> rk-win-vm-01	448K
<input type="checkbox"/> rk-win-vm-02	448K
<input type="checkbox"/> rk-vm-00	302K
<input type="checkbox"/> rk-cent-vm-01	301K
<input type="checkbox"/> rk-vm-02	293K

[+] More

Apply **Cancel**

⌵ Show legacy language converter

Perf
| where (Computer == "rk-win-vm-01")



Advanced Analy

00:00:00

449K Results [List](#) [Table](#)

2/16/2018 12:28:09.060 PM | Perf

... [Computer](#) : rk-win-vm-01
... [ObjectName](#) : System
... [CounterName](#) : Processor Queue Length
... [CounterValue](#) : 0
... [TimeGenerated](#) : 2/16/2018 12:28:09.060 PM
... [CounterPath](#) : \\rk-win-vm-01\System\Processor Queue Length
... [Computer_CPU](#) : 01

[\[+\] show more](#)

2/16/2018 12:28:09.060 PM | Perf

We can also do filtering from here

Perf
| where (Computer == "rk-win-vm-01")

449K Results [List](#) [Table](#)

2/16/2018 12:28:09.060 PM | Perf

... [Computer](#) : rk-win-vm-01

... [ObjectName](#) : System

... [Filter 'CounterName' to 'Processor Queue Length'](#)

Group by 'CounterName'

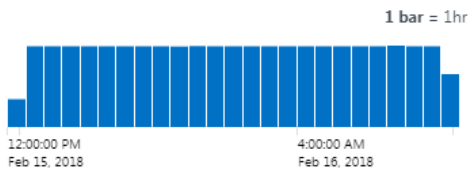
Show references to 'Processor Queue Length'

Add 'CounterName' to filters

Extract fields from 'Perf' (Preview)

Take action on 'Perf' (Preview)

Data based on last 1 day



TYPE (1)

Perf

x

9K

OBJECTNAME (1)

System

x

9K

COUNTERNAME (1)

x

[+Add](#)

[Show legacy language converter](#)

Perf
| where (Computer == "rk-win-vm-01")
| where CounterName == "Processor Queue Length"

9K Results [List](#) [Table](#)

2/16/2018 12:28:09.060 PM | Perf

... [Computer](#) : rk-win-vm-01

... [ObjectName](#) : System

... [CounterName](#) : Processor Queue Length

... CounterValue : 0

... TimeGenerated : 2/16/2018 12:28:09.060 PM

... [CounterPath](#) : \\rk-win-vm-01\System\Processor Queue Length

... [Computer_CF](#) : 01

[\[+\] show more](#)

2/16/2018 12:28:19.103 PM | Perf

```
Perf
| where ( Computer == "rk-win-vm-01" )
| where CounterName == "Processor Queue Length"|render table
```



Advanced Analytics

9K Results [List](#) [Table](#)

00:00:00.913

Drag a column header and drop it here to group by that column

	TimeGenerated	Computer	CounterName	Computer_CF	Counter
▶	2/16/2018 12:28:09.060 PM	rk-win-vm-01	Processor Queue Length	01	0
▶	2/16/2018 12:28:19.103 PM	rk-win-vm-01	Processor Queue Length	01	0
▶	2/16/2018 12:28:29.117 PM	rk-win-vm-01	Processor Queue Length	01	0
▶	2/16/2018 12:28:39.137 PM	rk-win-vm-01	Processor Queue Length	01	0
▶	2/16/2018 12:28:49.167 PM	rk-win-vm-01	Processor Queue Length	01	1

Another query which reports errors in syslog for a particular VM

Syslog

```
|where SeverityLevel == "err"
```

```
| where Computer == "rk-cent-vm-01"
```

Log Search

rk-oms-wrksp-prj

[Refresh](#)
[★ Saved Searches](#)
[Analytics](#)
[+ New Alert Rule](#)
[Export](#)
[PowerBI](#)

Data based on last 1 day

1 bar = 1hr

2:00:00 PM Feb 15, 2018

TYPE (1)

Syslog 4

HOSTNAME (1)

rk-cent-vm-01 4

[Show legacy language converter](#)

```
Syslog
|where SeverityLevel == "err"
| where Computer == "rk-cent-vm-01"
```

Advanced Analytics

00:00:00.476

4 Results [List](#) [Table](#)

2/16/2018 6:40:58.850 AM | Syslog

TimeGenerated

: 2/16/2018 6:40:58.850 AM

Computer

: rk-cent-vm-01

Facility

: syslog

HostName

: rk-cent-vm-01

SeverityLevel

: err

SyslogMessage

: imjournal: journal reloaded... [v8.24.0 try http://www.rsyslog.com/e/0]

[\[+\] show more](#)

Here is how processor time looks like

Perf

| where ObjectName=="Processor" and CounterName=="% Processor Time"

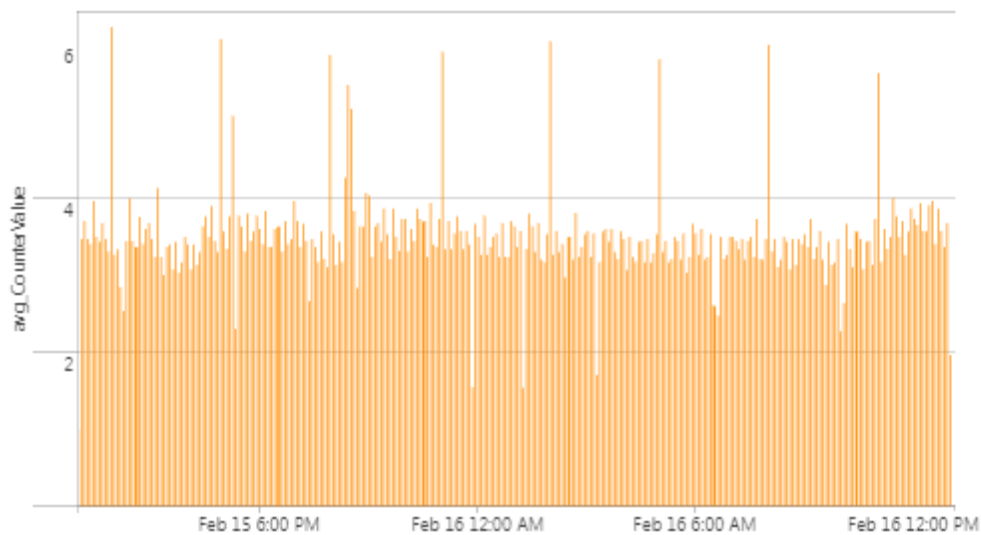
| where Computer == "rk-ubt-vm-01" | summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)|render barchart

Perf

| where ObjectName=="Processor" and CounterName=="% Processor Time"

| where Computer == "rk-ubt-vm-01" | summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)|render barchart

289 Results [Chart](#) [Table](#)



[SELECT ALL](#) [SELECT NONE](#)

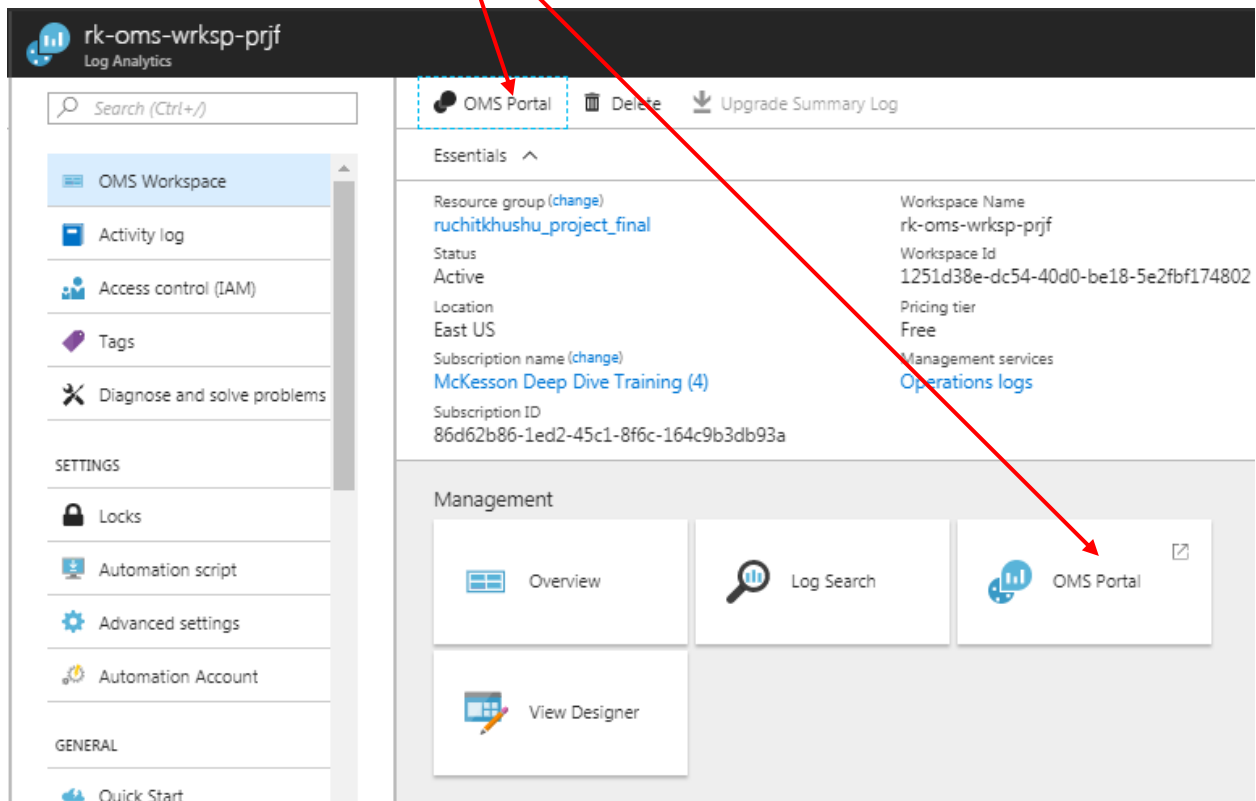
■ rk-ubt-vm-01

Next we will create some alerts and dashboard

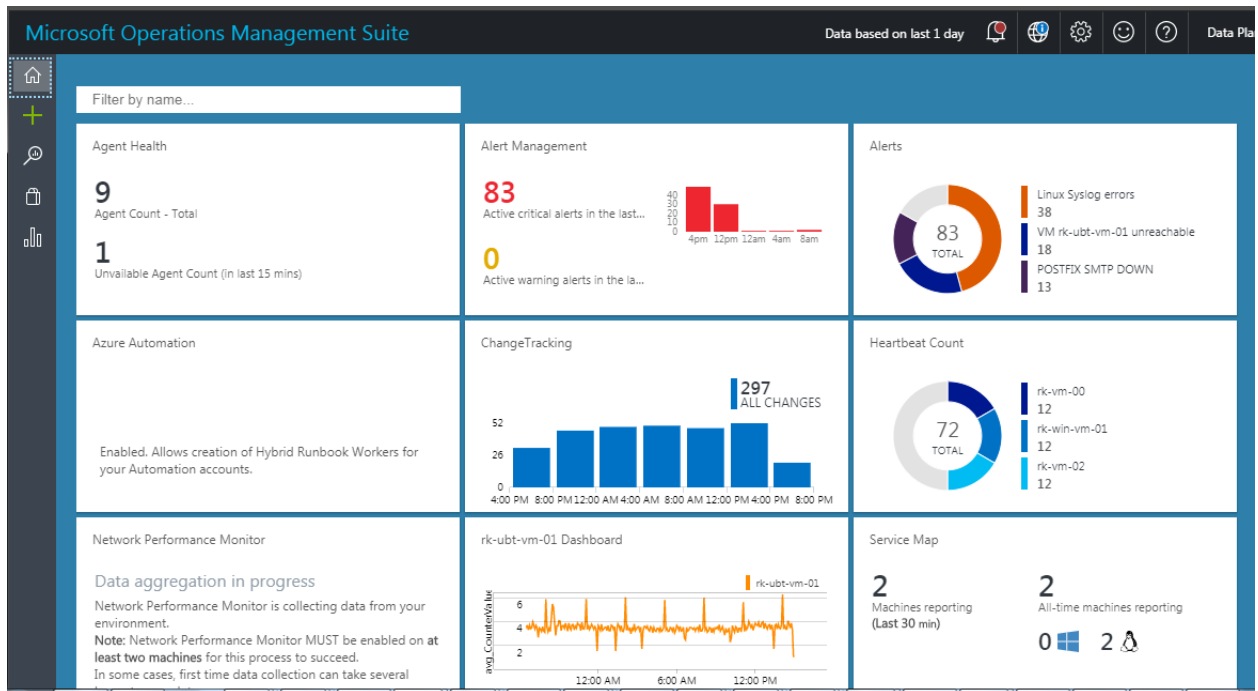
OMS Portal

OMS Portal is dedicated portal for OMS activities. We can practically do most of things we do in OMS portal in Azure portal itself however for a few things like Dashboard creation and Solutions

We can go from Overview to OMS Portal

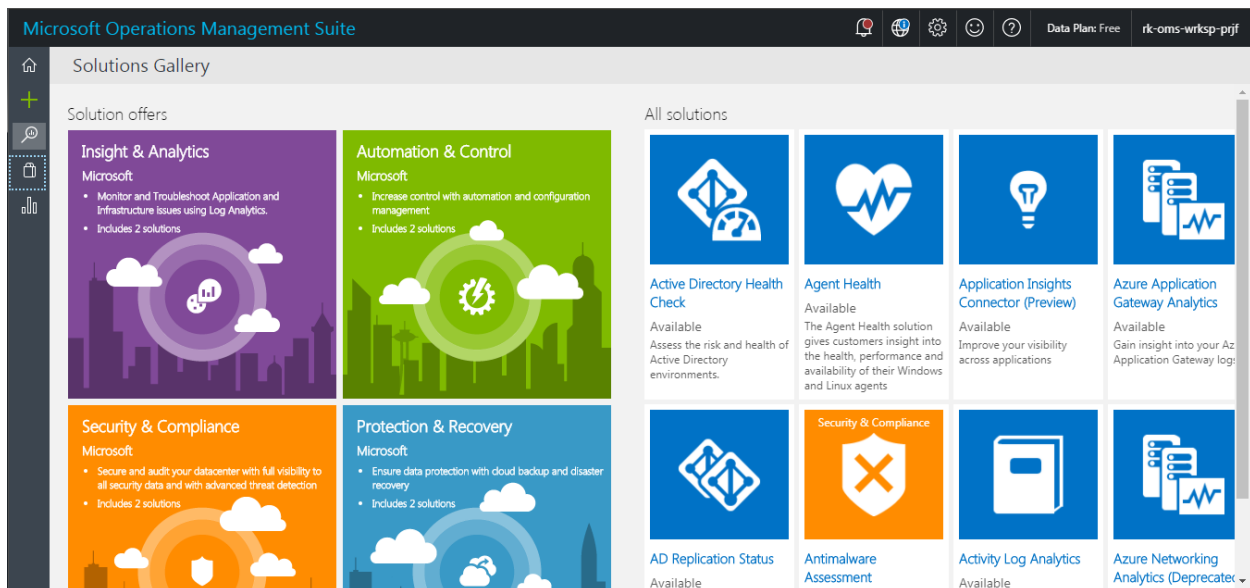


OMS portal url is : <https://<OMS-workspacename>.portal.mms.microsoft.com/>

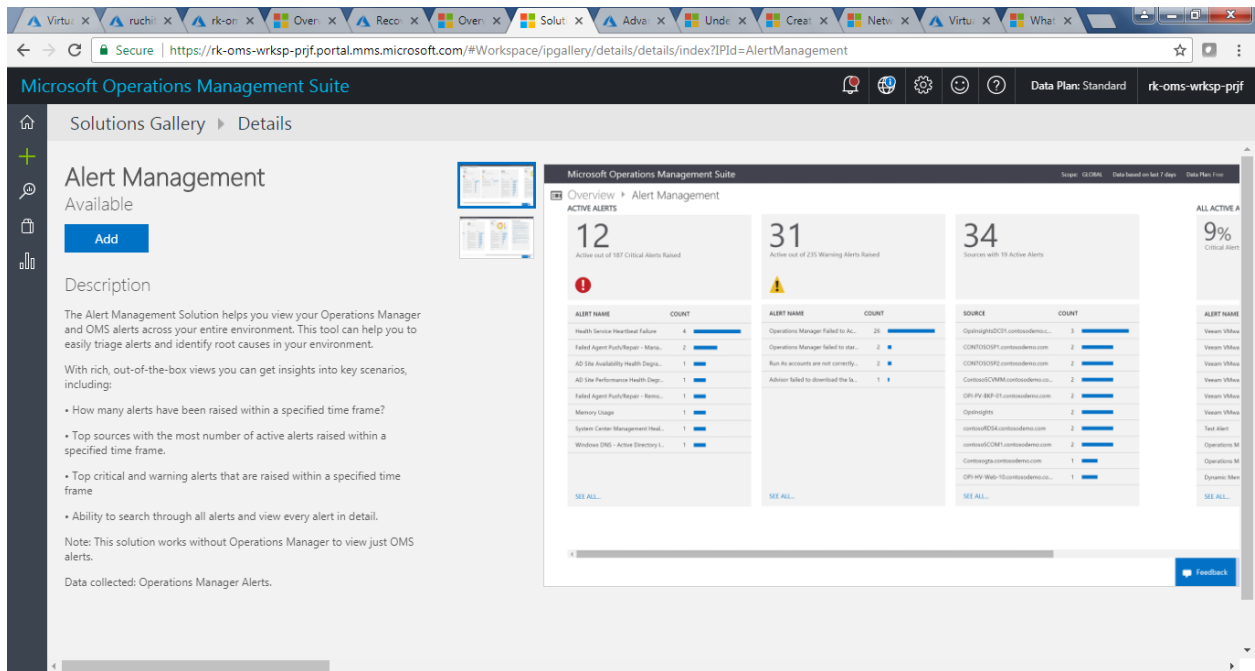


Add Solutions using OMS Portal

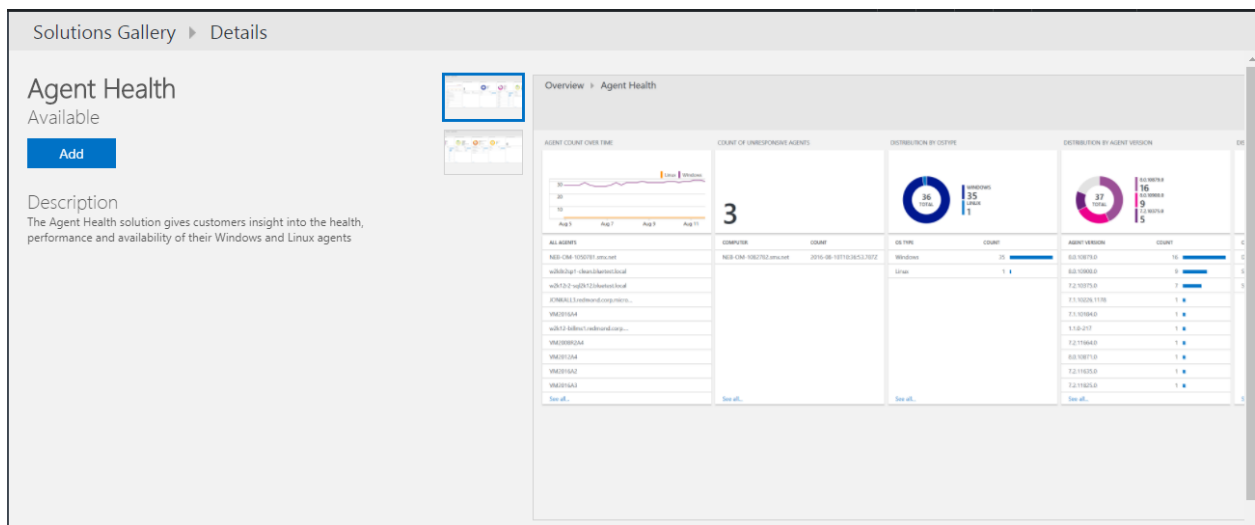
Inside the OMS portal you can choose ready to be deployed solution from Solution Gallery



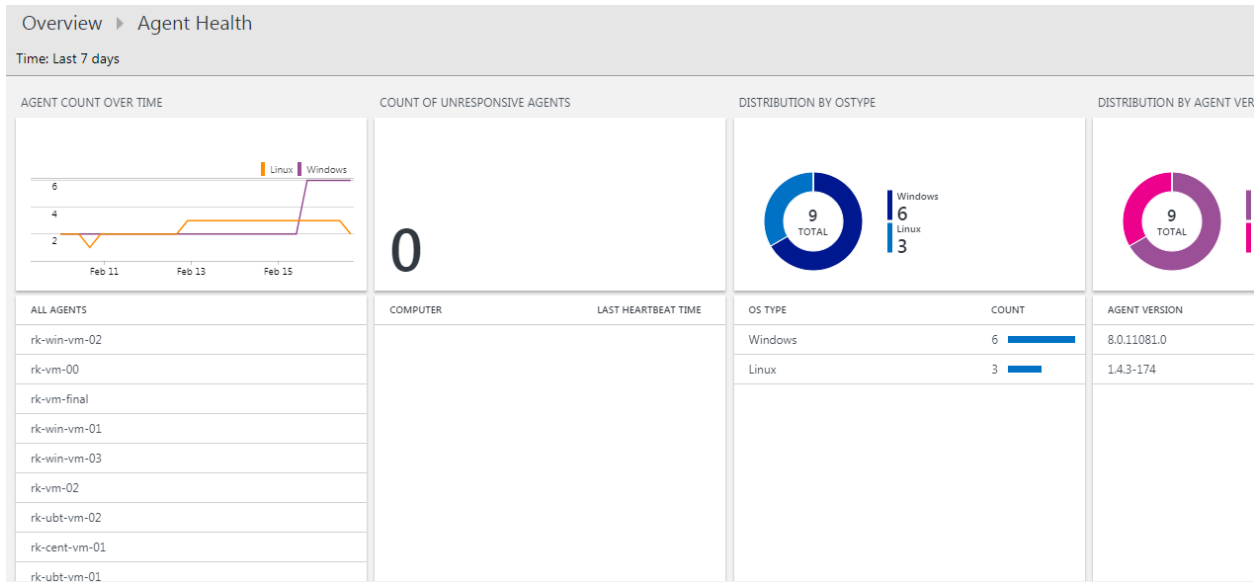
I deployed Alert Monitoring and Change Management manually . To deploy any solution we have double click on it and follow the instructions .



Here is example of how to add one of solutions: Agent Health



After deploying when I get inside the Solution dashboard this is what I see



Create custom Dashboards in OMS Portal

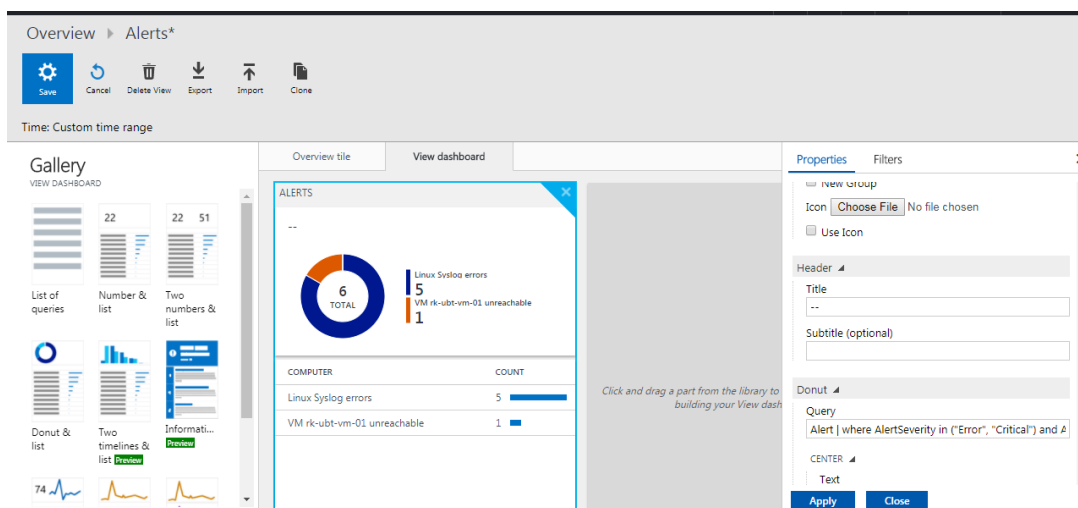
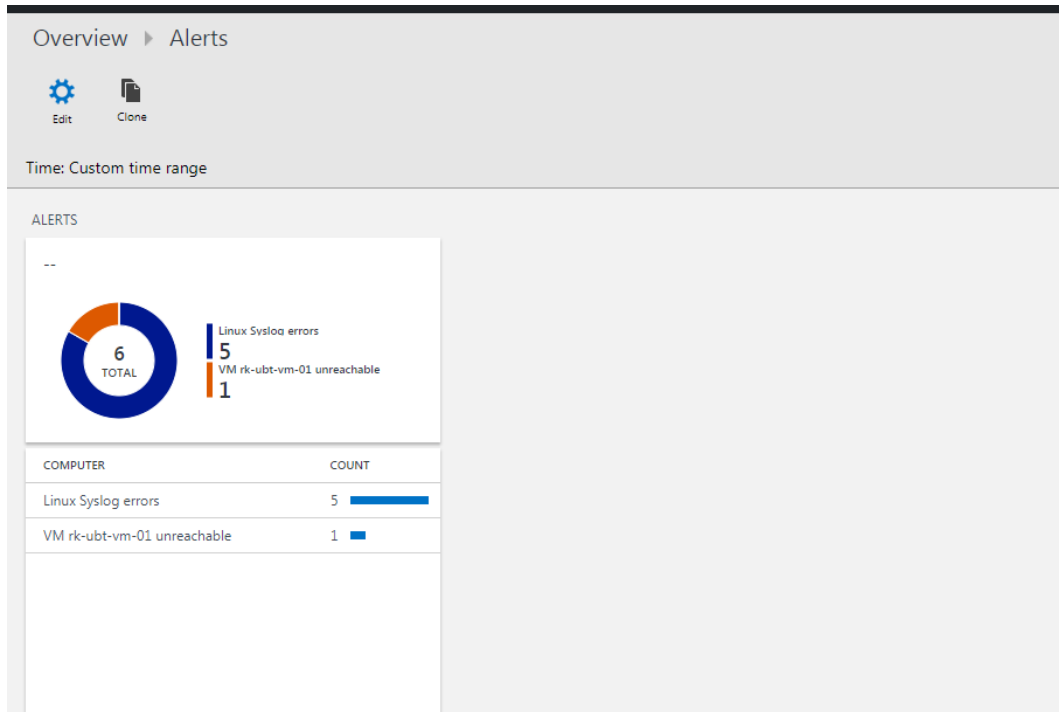


Some of the dashboards that you see in the screen above are standard dashboards that get imported with Solution Imports. The others we a custom dashboards. To create a new dashboard view you need to click on the Green plus button

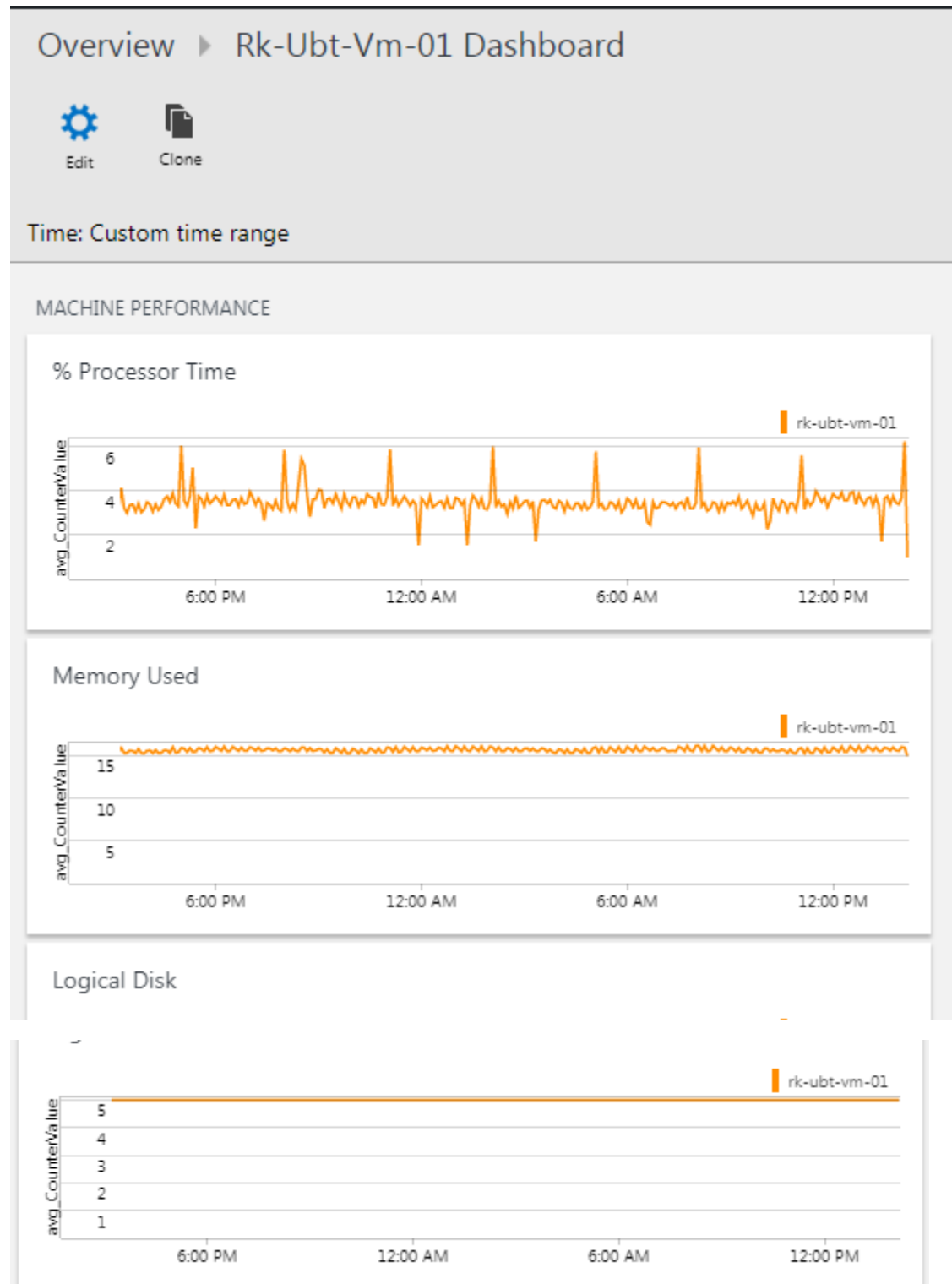
I created 2 custom dashboards as part of the project – One for Performance metrics of one of the VMs one for Heart beats and other one for Alert Management [

Alert Management Dashboard

The query I used was: Alert | where AlertSeverity in ("Error", "Critical") and AlertState != "Closed" | summarize Count = count() by AlertName



Performance dashboard for VM

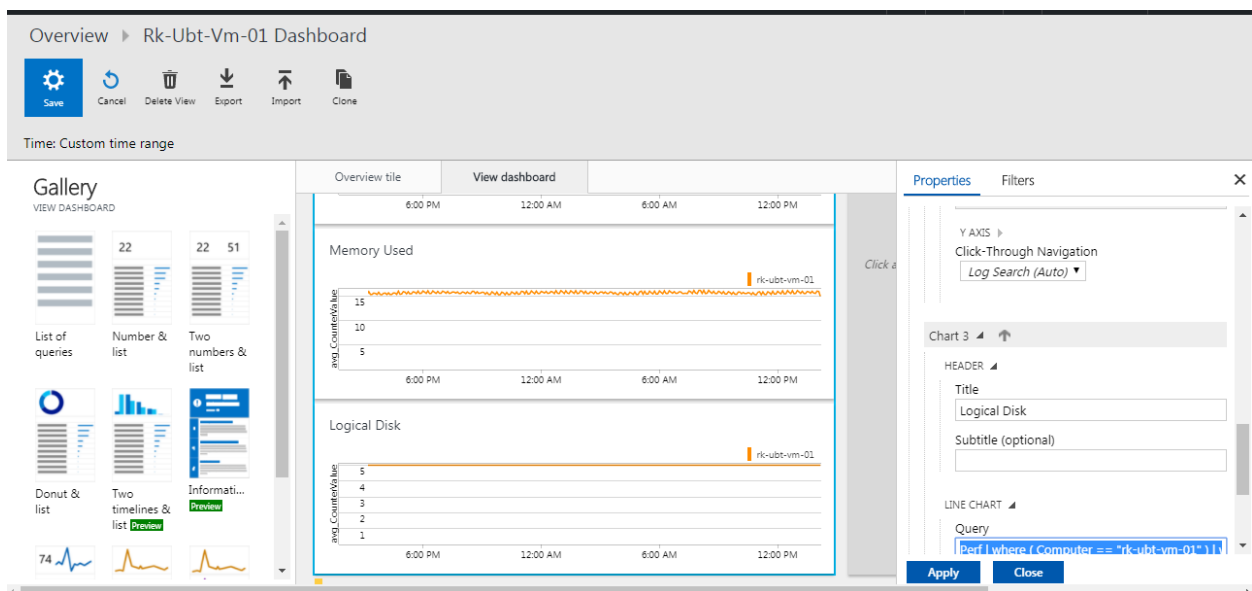


I used these queries

Perf | where ObjectName=="Processor" and CounterName=="% Processor Time" | where Computer == "rk-ubt-vm-01" | summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)|render barchart

Perf | where ObjectName == "Memory" and CounterName == "% Used Memory" | where Computer == "rk-ubt-vm-01" | summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)|render barchart

Perf | where (Computer == "rk-ubt-vm-01") | where (ObjectName == "Logical Disk") | where (CounterName == "% Used Space") | summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)|render barchart



Alerts:

One of big advantages that Log Analytics provides is to set up Alerts . We can set up Alerts based on the output of the log queries.

In order to create a new Alert please go the OMS Portal and in the log search section input the query for which Alerts needs to created

The screenshot displays the Microsoft Operations Management Suite (OMS) Log Search interface. The top navigation bar includes the OMS logo, user profile, and data plan information. The left sidebar contains icons for Log Search, Favorites, History, and Analytics. The main content area shows a search bar with the text 'syslog' and a 'Convert' button. Below the search bar, a query is entered: 'Syslog | where SeverityLevel == "err" | search "processmon error missing /usr/lib/postfix/sbin/master"'. The results section shows 26 results, with a table view displaying details for a specific log entry. A red arrow points to the 'Alert' button in the top navigation bar.

Click on the Alert button..On the next screen fill in the information...

Log Search ► Add Alert Rule

General

Alert information

Name
PO

Description

Severity
Critical

Search query
Use current search query

Syslog
|where SeverityLevel == "err"
| search "processmon error missing
/usr/lib/postfix/sbin/master"

Save Cancel

Schedule

Alert frequency
Check for this alert every
15 Minutes

Generate alert based on
Number of results Metric measurement

Number of results
Greater than Eg: 100
Threshold should be a positive integer between 0 and 10000

☐ Suppress alerts
When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Actions

☒ Email notification
Yes No

Subject
Email subject

Recipients (semi-colon separated)
Ruchit.Khushu@McKesson.com

☒ Webhook
Yes No

☒ Runbook
Yes No

☒ ITSM Actions

Log Search ► Add Alert Rule

General

Alert information

Name
PostFIX SMTP DOWN

Description
PostFIX SMTP down on VM tk-ub-vm-01

Severity
Critical

Search query
Use current search query

Syslog
|where SeverityLevel == "err"
| search "processmon error missing
/usr/lib/postfix/sbin/master"

Save Cancel

Schedule

Alert frequency
Check for this alert every
10 Minutes

Generate alert based on
Number of results Metric measurement

Number of results
Greater than 0

☐ Suppress alerts
When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Actions

☒ Email notification
Yes No

Subject
PostFIX SMTP down on tk-ub-vm-01

Recipients (semi-colon separated)
Ruchit.Khushu@McKesson.com

☒ Webhook
Yes No

☒ Runbook
Yes No

☒ ITSM Actions

And Save !!

If you check the Alert(Preview) section under OMS Workspace you will get a list of all the Alerts created. Alternatively you can also view them inside the OMS portal by selection Settings and then go Alert tab.

rk-oms-wrksp-prjf - Alerts (Preview)
Log Analytics

Search (Ctrl+/)

GENERAL

Quick Start

Overview

View Designer

Log Search

Solutions

Pricing tier

Retention

Log Analytics usage

Properties

Saved searches

Upgrade Summary

Alerts (Preview)

Service Map

WORKSPACE DATA SOURCES

Columns Refresh + New Alert Rule Enable Disable Delete

* Subscription ⓘ

Resource group ⓘ

Resource ⓘ

McKesson Deep Dive Training (...)

ruchitkhushu_project_final

rk-oms-wrksp-prjf

McKesson Deep Dive Training (4) > ruchitkhushu_project_final > rk-oms-wrksp-prjf

7 Rules | 7 Enabled

Filter alerts...

<input type="checkbox"/>	NAME	CONDITION	STATUS	TARGET RESO...
<input type="checkbox"/>	VM rk-ubt-vm-01 unreac...	Heartbeat where (Computer == "rk-ubt-vm-...	Enabled	rk-oms-wrksp-prjf
<input type="checkbox"/>	VM rk-win-vm-02 unreac...	Heartbeat where (Computer == "rk-win-vm-...	Enabled	rk-oms-wrksp-prjf
<input type="checkbox"/>	Linux Syslog errors	Syslog where SeverityLevel == "err"	Enabled	rk-oms-wrksp-prjf
<input type="checkbox"/>	VM rk-win-vm-01 unreac...	Heartbeat where (Computer == "rk-win-vm-...	Enabled	rk-oms-wrksp-prjf
<input type="checkbox"/>	VM rk-ubt-vm-02 unreac...	Heartbeat where (Computer == "rk-ubt-vm-...	Enabled	rk-oms-wrksp-prjf
<input type="checkbox"/>	POSTFIX SMTP DOWN	Syslog where SeverityLevel == "err" search "...	Enabled	rk-oms-wrksp-prjf
<input type="checkbox"/>	Unexpected shutdown o...	Event where EventLog == 'System' and EventL...	Enabled	rk-oms-wrksp-prjf

Custom Alerts

As part of this project I created a whole of alerts mainly dealing with VM and Process monitoring..

For VM availability monitoring I used heart beat log type.

Heartbeat Monitoring

For example for one of my VMs the query was: **Heartbeat | where (Computer == "rk-ubt-vm-01").** I created an Alert for this as shown below:

Overview ► Settings ► Edit Alert Rule

General

Alert information

Name
VM rk-ubt-vm-01 unreachable

Description
Can't find heartbeat of rk-ubt-vm-01

Severity
Critical

Search query
Alertlbiza : VM rk-ubt-vm-01 unreachable
Heartbeat
| where (Computer == "rk-ubt-vm-01")

Schedule

Alert frequency
Check for this alert every
6 Minutes

Generate alert based on
Number of results
Less than 1

☐ Suppress alerts
When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Actions

Email notification
Yes No

Subject
VM rk-ubt-vm-01 unreachable

Recipients (semi-colon separated)
Ruchit.Khushu@McKesson.com


Webhook
Yes No

Runbook
Yes No

Save Cancel


Next when I shut down the VM I got an e-mail alert..I actually got a lot of them and if you want to suppress that use the Suppress Alerts feature..

Delete
Respond
Quick Steps
1x
Move


Microsoft Operations Management Suite Team <noreply@oms.microsoft.com>
Kushu, Ruchit

VM rk-ubt-vm-01 unreachable

Retention Policy FLD - Inbox Delete after 90 Days (90 days) Expires 5/17/2018

 If there are problems with how this message is displayed, click here to view it in a web browser.

We are notifying you because there are 0 counts of "VM rk-ubt-vm-01 reachable"

NAME	VM rk-ubt-vm-01 reachable
SEVERITY	Critical
WORKSPACE NAME	rk-oms-wrksp-prjf
SEARCH INTERVAL START TIME	2/17/2018 12:41:33 AM (UTC)
SEARCH INTERVAL DURATION	6 min
SEARCH QUERY	Heartbeat where (Computer == "rk-ubt-vm-01")
SEARCH RESULTS	0 result(s)
DESCRIPTION	Can't find heartbeat of rk-ubt-vm-01

Top 10 result(s)

I also set up two alerts for Process/Service Monitoring

Linux Service Monitoring

On one of VMs I installed a simple lightweight Postfix SMTP relay server. I subsequently created a shell script that would keep on checking every 5 mins if the postfix process was running or not. If not it will write a error message to syslog. Then I created an Alert for checking for this error line in syslog and I even a single count was found alert would be triggered.

The query I used is:

Syslog


/where SeverityLevel == "err"

/ search "processmon error missing /usr/lib/postfix/sbin/master"


"processmon error missing /usr/lib/postfix/sbin/master" is the line that gets run to the syslog !!

General	Schedule	Actions
Alert information Name <input type="text" value="POSTFIX SMTP DOWN"/> Description <input type="text" value="PostFIX SMTP down on VM rk-ub-vm-01"/> Severity <input type="text" value="Critical"/> Search query <input type="text" value="Alert : POSTFIX SMTP DOWN"/> <pre>Syslog where SeverityLevel == "err" search "processmon error missing /usr/lib/postfix/sbin/master"</pre>	Alert frequency Check for this alert every <input type="text" value="10"/> <input type="text" value="Minutes"/> Generate alert based on <input checked="" type="button" value="Number of results"/> <input type="button" value="Metric measurement"/> Number of results <input type="text" value="Greater than"/> <input type="text" value="0"/> <input type="checkbox"/> Suppress alerts <small>When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise</small>	Email notification <input checked="" type="button" value="Yes"/> <input type="button" value="No"/> Subject <input type="text" value="PostFIX SMTP down on rk-ub-vm-01"/> Recipients (semi-colon separated) <input type="text" value="Ruchit.Khushu@McKesson.com"/> Webhook <input type="button" value="Yes"/> <input checked="" type="button" value="No"/> Runbook <input type="button" value="Yes"/> <input checked="" type="button" value="No"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

And this is the email alert


PostFIX SMTP down on rk-ub-vm-01

Retention Policy: FLD - Inbox Delete after 90 Days (90 days) Expires: 5/17/2018

 If there are problems with how this message is displayed, click here to view it in a web browser.

We are notifying you because there are 1 counts of "POSTFIX SMTP DOWN"

NAME	POSTFIX SMTP DOWN
SEVERITY	Critical
WORKSPACE NAME	rk-oms-wrksp-prjf
SEARCH INTERVAL START TIME	2/17/2018 12:44:21 AM (UTC)
SEARCH INTERVAL DURATION	10 min
SEARCH QUERY	Syslog where SeverityLevel == "err" search "processmon error missing /usr/lib/postfix/sbin/master"
SEARCH RESULTS	1 result(s)
DESCRIPTION	PostFIX SMTP down on VM rk-ub-vm-01

Top 10 result(s)

I have put the Linux shell script on Github as [linuxprocmon.sh](#)

MS-SQL Server Down

I installed MS-SQL Server on one of the VMs and then wrote a PowerShell script that checks if the services are running or not and if not write an error message to Application log.

And then I created an alert that queries the application event log

Overview ► Settings ► Edit Alert Rule

General

Alert information

Name
MSSQ Server Down

Description
MSSQL server is down

Severity
Critical

Search query
Alert : MSSQ Server Down

search (Type == "Event")
| where (EventLevelName == "Error")
| search "Service MSSQL\$DEEPAZURE is down"

Save Cancel

Schedule

Alert frequency
Check for this alert every
10 Minutes

Generate alert based on
Number of results Metric measurement

Number of results
Greater than 1

☐ Suppress alerts
When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Actions

☒ Email notification

Yes No

Subject
MSSQL server is down

Recipients (semi-colon separated)
Ruchit.Khushu@McKesson.com

☒ Webhook

Yes No

☒ Runbook

Yes No

The following is the power shell script I built for this . It has to be run on the machine for which the monitoring has to be performed using Task scheduler . ***I have put the this service monitor power shell script on Github as [winsvcmon.sh](#)***

```
$file = $args[0];
Import-CSV $file | ForEach-Object {

$MYNAME = $_.Name
$TYPE = $_.Type

if ($Type -eq 'Service') {

$ServiceDetails = Get-Service -Name $MYNAME
if ($ServiceDetails.Status -ne "Running"){

Write-EventLog -LogName "Application" -Source $MYNAME -EventID 1 -EntryType Error -
Message "$TYPE $MYNAME is down." -Category 1 -RawData 10,20
}
}
```

```

}

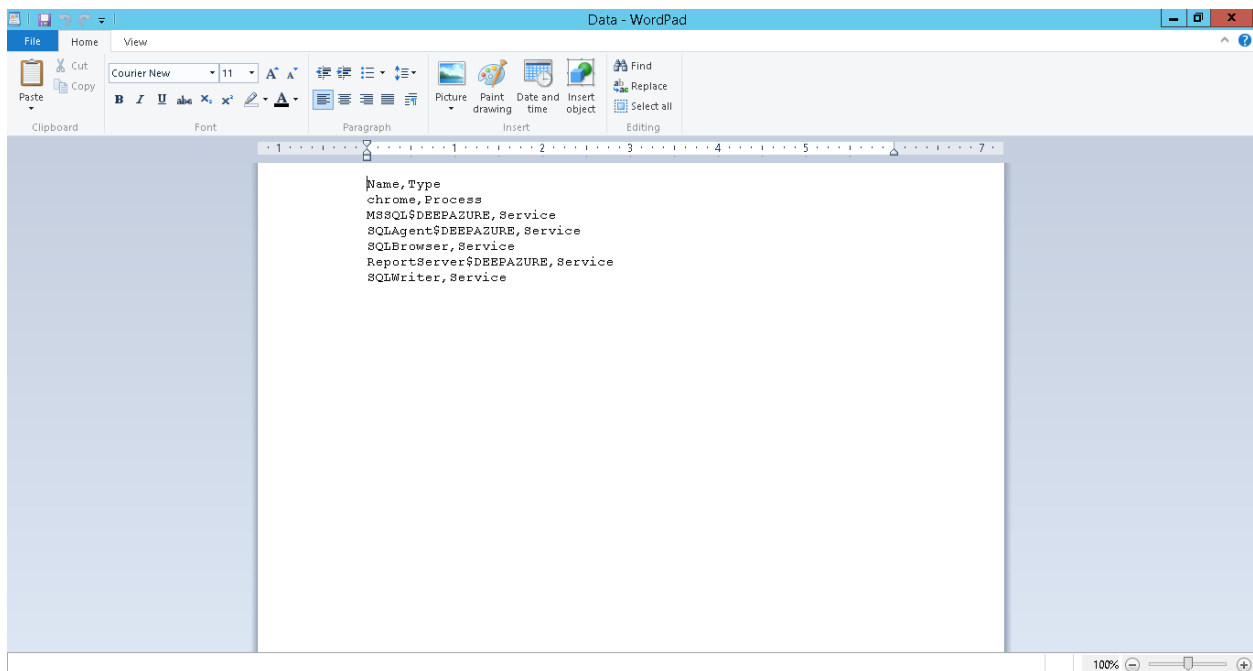
elseif ($TYPE -eq "Process") {

$ProcessDetails = Get-Process -Name $MYNAME -ErrorAction SilentlyContinue
if (!$ProcessDetails) {

Write-EventLog -LogName "Application" -Source $MYNAME -EventID 1 -EntryType Error -
Message "$TYPE $MYNAME is down." -Category 1 -RawData 10,20
}
}
}

```

The data file with service names can look like this:



Service Map:

I also enabled Service Maps For this I deployed the Service MAP Solution from OMS Gallery

The screenshot displays the Microsoft Operations Management Suite (OMS) interface. On the left, the 'Service Map' solution is listed as 'Available' with an 'Add' button. Below this, a description states: 'Service Map presents a view of your servers as you think of them - as interconnected systems that deliver services and rely on other technologies. Service Map discovers and maps server and process dependencies in real-time, without any predefinition, and visualizes application components, service dependencies, and supporting infrastructure configuration. This helps you eliminate the guesswork of problem isolation, identify surprise connections and broken links in your environment, and perform Azure migrations knowing that critical systems and endpoints won't be left behind. Service Map supports Windows and Linux guests, for any cloud and on-prem.' It also mentions 'Diagnostic and Usage Data' and provides a link to the 'Microsoft Online Services Privacy Statement'.

The main part of the screenshot shows the 'Overview - Service Map' view. It features a visual dependency map with nodes representing servers and processes, connected by lines indicating dependencies. On the right, there are several performance charts for 'adrdemo-appegr' and 'adrdemo-appegr' showing CPU utilization, memory utilization, and network I/O over time. A table at the bottom right lists 'Processes that received data' with columns for name, size, and count.

And then deployed the Linux Dependency Agent on 1 on UBUNTU and 1 of my CENTOS VMs.

```
root@rk-ubt-vm-02: ~/Linux-Dependency-Agent
root@rk-ubt-vm-02:~# mkdir Linux-Dependency-Agent
root@rk-ubt-vm-02:~# cd Linux-Dependency-Agent
root@rk-ubt-vm-02:~/Linux-Dependency-Agent# vi LDA.sh
You have new mail in /var/mail/root
```

I created LDA.sh script with installation instructions

```
root@rk-ubt-vm-02: ~/Linux-Dependency-Agent
/bin/bash
wget --content-disposition https://aka.ms/dependencyagentlinux -O InstallDependencyAgent-Linux64.bin
sudo sh InstallDependencyAgent-Linux64.bin -s
```

Script execution resulted in the installion of the Agent

```

- Installation
- Installing to /lib/modules/4.4.0-47-generic/updates/dkms/

bluechannel.ko:
Running module version sanity check.
- Original module
- No original module exists within this kernel
- Installation
- Installing to /lib/modules/4.4.0-47-generic/updates/dkms/

depmod.....

DKMS: install completed.
Building initial module for 4.4.0-112-generic
Done.

microsoft-dependency-agent:
Running module version sanity check.
- Original module
- No original module exists within this kernel
- Installation
- Installing to /lib/modules/4.4.0-112-generic/updates/dkms/

bluechannel.ko:
Running module version sanity check.
- Original module
- No original module exists within this kernel
- Installation
- Installing to /lib/modules/4.4.0-112-generic/updates/dkms/

depmod....

DKMS: install completed.
Setting up dependency-agent-service (9.4.1-1134) ...
Loading Microsoft Dependency Agent driver done.
Microsoft Dependency Agent service started.
Processing triggers for systemd (229-4ubuntu21.1) ...
Processing triggers for ureadahead (0.100.0-19) ...
Core Agent installation complete.

Dependency Agent installation was successful.
Refer to the logs under /var/opt/microsoft/dependency-agent/log for details.
You have new mail in /var/mail/root
root@rk-ubt-vm-02:~/Linux-Dependency-Agent# █

```

```

root@rk-ubt-vm-02:~/Linux-Dependency-Agent# ps -ef|grep microsoft-dependency-agent
root      78454      1  0 06:43 pts/0    00:00:00 /bin/sh /opt/microsoft/dependency-agent/bin/microsoft-dependency-agent-manager
root      78504  78454  0 06:43 pts/0    00:00:00 /opt/microsoft/dependency-agent/bin/microsoft-dependency-agent
root      78612  67975  0 06:44 pts/0    00:00:00 grep --color=auto microsoft-dependency-agent
root@rk-ubt-vm-02:~/Linux-Dependency-Agent# █

```



```

root@rk-cent-vm-01:~/Linux-Dependency-Agent
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 ~]# pwd
/root
[root@rk-cent-vm-01 ~]# mkdir Linux-Dependency-Agent
[root@rk-cent-vm-01 ~]# cd Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# vi LDainstall.sh
[root@rk-cent-vm-01 Linux-Dependency-Agent]# chmod 755 LDainstall.sh
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 Linux-Dependency-Agent]# ./LDainstall.sh

```

```

root@rk-cent-vm-01:~/Linux-Dependency-Agent
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 ~]# pwd
/root
[root@rk-cent-vm-01 ~]# mkdir Linux-Dependency-Agent
[root@rk-cent-vm-01 ~]# cd Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# vi LDainstall.sh
[root@rk-cent-vm-01 Linux-Dependency-Agent]# chmod 755 LDainstall.sh
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 Linux-Dependency-Agent]# ./LDainstall.sh
--2018-02-13 08:33:35-- https://aka.ms/dependencyagentlinux
Resolving aka.ms (aka.ms)... 23.14.181.100
Connecting to aka.ms (aka.ms)[23.14.181.100]:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://download.microsoft.com/download/E/D/B/EDB22276-C316-4982-AFED-6367255D0824/InstallDependencyAgent-Linux64.bin [following]
--2018-02-13 08:33:36-- http://download.microsoft.com/download/E/D/B/EDB22276-C316-4982-AFED-6367255D0824/InstallDependencyAgent-Linux64.bin
Resolving download.microsoft.com (download.microsoft.com)... 23.44.160.32, 2600:1406:40:2bf::e59, 2600:1406:40:2ac::e59
Connecting to download.microsoft.com (download.microsoft.com)[23.44.160.32]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18256154 (17M) [application/octet-stream]
Saving to: 'InstallDependencyAgent-Linux64.bin'

100%[=====>] 18,256,154 16.8MB/s in 1.0s

2018-02-13 08:33:37 (16.8 MB/s) - 'InstallDependencyAgent-Linux64.bin' saved [18256154/18256154]

Dependency Agent 9.4.1.1134 Setup for Linux
=====
Checking installation environment...
No old version of the Dependency Agent found. Performing fresh installation.

```

```
[root@rk-cent-vm-01 ~]# pwd
/root
[root@rk-cent-vm-01 ~]# mkdir Linux-Dependency-Agent
[root@rk-cent-vm-01 ~]# cd Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# vi LDAinstall.sh
[root@rk-cent-vm-01 Linux-Dependency-Agent]# chmod 755 LDAinstall.sh
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 Linux-Dependency-Agent]# ./LDAinstall.sh
--2018-02-13 08:33:35-- https://aka.ms/dependencyagentlinux
Resolving aka.ms (aka.ms)... 23.14.161.100
Connecting to aka.ms (aka.ms)|23.14.161.100|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://download.microsoft.com/download/E/D/B/EDB22276-C316-4982-AFED-6367255D0824/InstallDependencyAgent-Linux64.bin [following]
--2018-02-13 08:33:36-- http://download.microsoft.com/download/E/D/B/EDB22276-C316-4982-AFED-6367255D0824/InstallDependencyAgent-Linux64.bin
Resolving download.microsoft.com (download.microsoft.com)... 23.44.160.32, 2600:1406:40:2bf::e59, 2600:1406:40:2ac::e59
Connecting to download.microsoft.com (download.microsoft.com)|23.44.160.32|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18256154 (17M) [application/octet-stream]
Saving to: âInstallDependencyAgent-Linux64.binâ

100%[=====>] 18,256,154 16.8MB/s in 1.0s

2018-02-13 08:33:37 (16.8 MB/s) - âInstallDependencyAgent-Linux64.binâ saved [18256154/18256154]

Dependency Agent 9.4.1.1134 Setup for Linux
=====

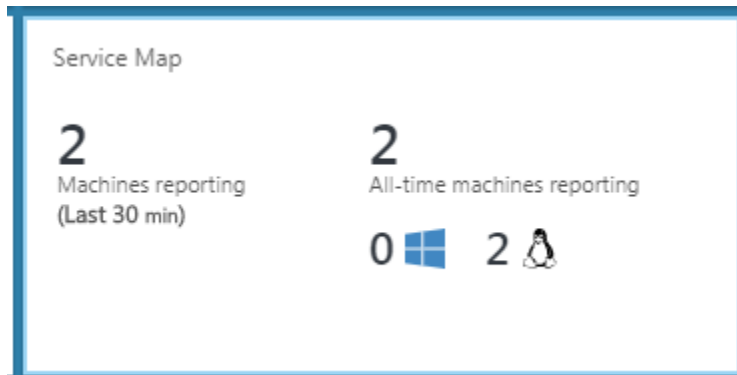
Checking installation environment...
No old version of the Dependency Agent found. Performing fresh installation.

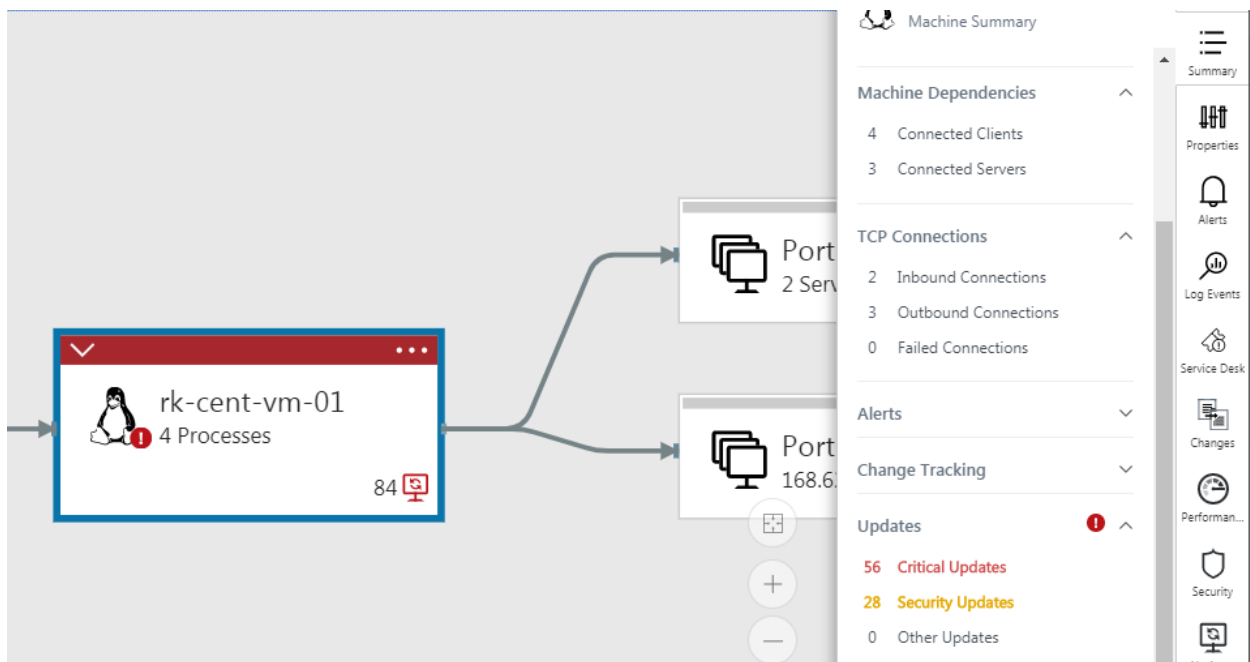
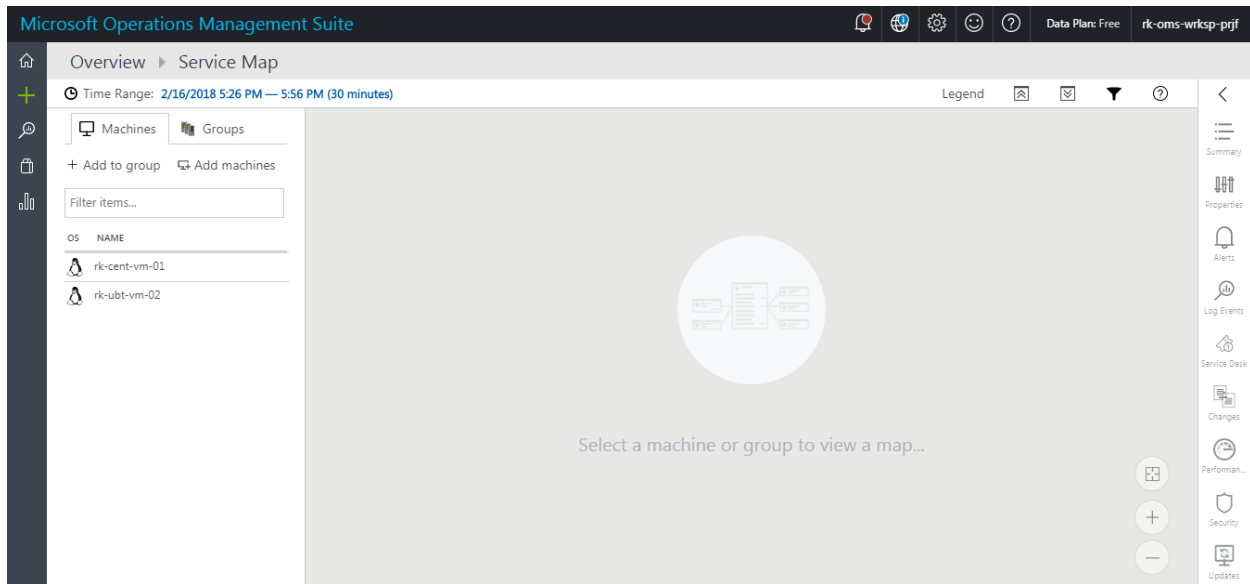
Extracting dependency-agent.rpm... checking md5... done.

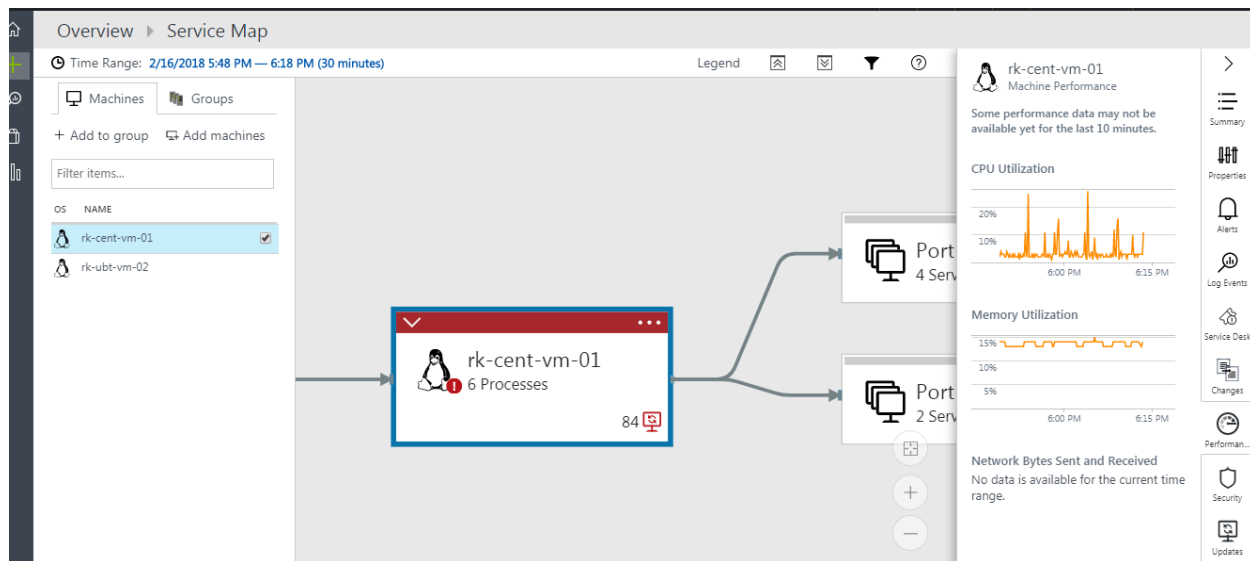
Preparing... ##### [100%]
Updating / installing...
 1:dependency-agent-9.4.1-1134 ##### [100%]
Loading Microsoft Dependency Agent driver done.
Microsoft Dependency Agent service started.
Core Agent installation complete.

Dependency Agent installation was successful.
Refer to the logs under /var/opt/microsoft/dependency-agent/log for details.
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 Linux-Dependency-Agent]#
```

```
root@rk-cent-vm-01~/.Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# ps -ef|grep microsoft/dependency-agent
root    36106      1  0 08:33 pts/0    00:00:00 /bin/sh /opt/microsoft/dependency-agent/bin/microsoft-dependency-agent-manager
root    36148    36106  0 08:33 pts/0    00:00:00 /opt/microsoft/dependency-agent/bin/microsoft-dependency-agent
root    36174    36148  0 08:33 pts/0    00:00:00 /opt/microsoft/omsagent/ruby/bin/ruby /opt/microsoft/dependency-agent/lib/plugins/AzureMetadata.rb
root    36227    34397  0 08:34 pts/0    00:00:00 grep --color=auto microsoft/dependency-agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]#
```







Summary

I was able to set up an OMS workspace, configure it and add virtual machines to be monitored to it.. I subsequently set up Alerts and created dashboard views as also deployed standard dashboards. I learnt a lot about Log query.. I fulfilled whatever I had set out to achieve.