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=tEIv9lbLDZg&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

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 VMnet-Complex.py


This script will create 2 Windows 2012 R2 VMs and 2 Ubuntu VMs along with necess
ary 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_Vnet............
-------------------------------------------------------
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Network/virtualNetworks/rk_VNet', 'nam
e': 'rk_VNet', '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/"beb4ed66-623e-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 0x0000000053B1C88>], 'dns_settings': <azure.mgmt.network.v2
017_03_01.models.network_interface_dns_settings.NetworkInterfaceDnsSettings obje
ct at 0x0000000053B1CC0>, '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 VM
------------------------------------------------------------
{'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 0x0000000053A9198>, 'storage_profile
': <azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storag
eProfile object at 0x0000000053A9828>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x0000000053A99E8>,
 'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x0000000050E0C88>, '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 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 0x0000000050C4E48>, 'storage_profile
': <azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storag
eProfile object at 0x0000000050C4940>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x0000000050C4198>,
 'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x0000000050C42E8>, '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...
```

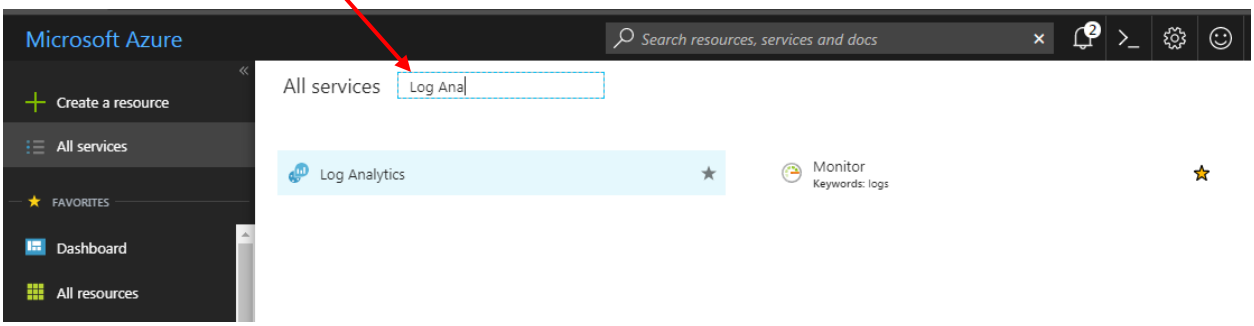
```
C:\windows\system32\cmd.exe - python VMnet-Complex.py
-------------------------------------------------------
Creating Windows VM
-------------------------------------------------------
{'id': '/subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourceGroups/ruchi
tkhushu_project_final/providers/Microsoft.Compute/virtualMachines/rk-win-vm-02',
 '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.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...

-------------------------------------------------------
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.Storag
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-bbed-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.Storag
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_vie
w': 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/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 0x0000000050C45F8>, 'storage_profile
': <azure.mgmt.compute.compute.v2016_04_30_preview.models.storage_profile.Storag
eProfile object at 0x0000000050C4898>, 'os_profile': <azure.mgmt.compute.comput
e.v2016_04_30_preview.models.os_profile.OSProfile object at 0x0000000050C4EF0>,
 'network_profile': <azure.mgmt.compute.compute.v2016_04_30_preview.models.netwo
rk_profile.NetworkProfile object at 0x0000000053B1668>, '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...

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

C:\myPython>_
```

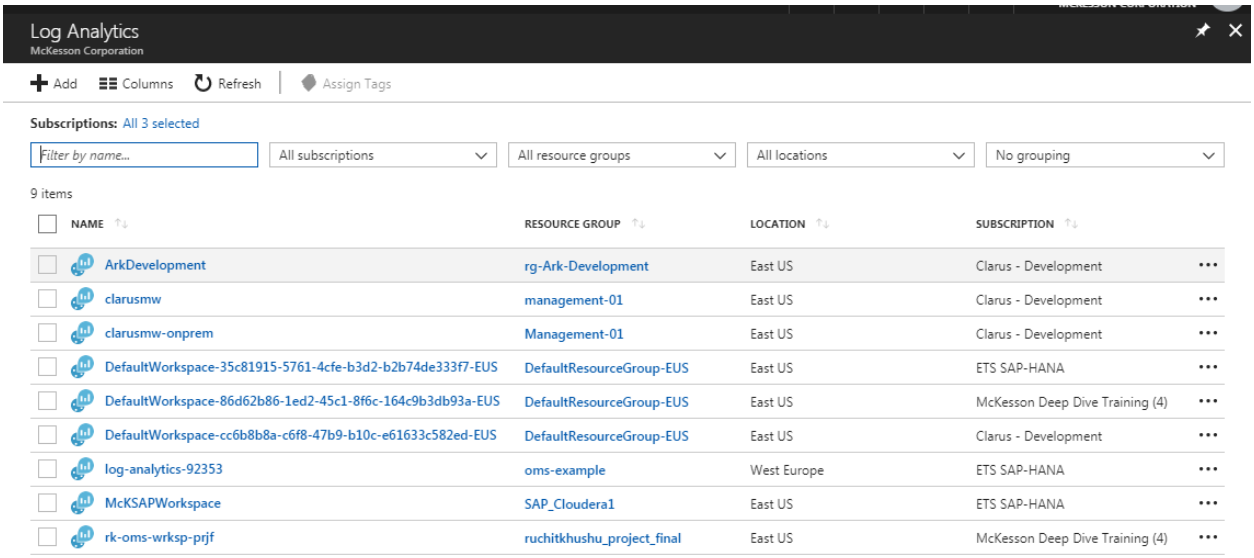
Creating OMS Workspace in Azure Portal:

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

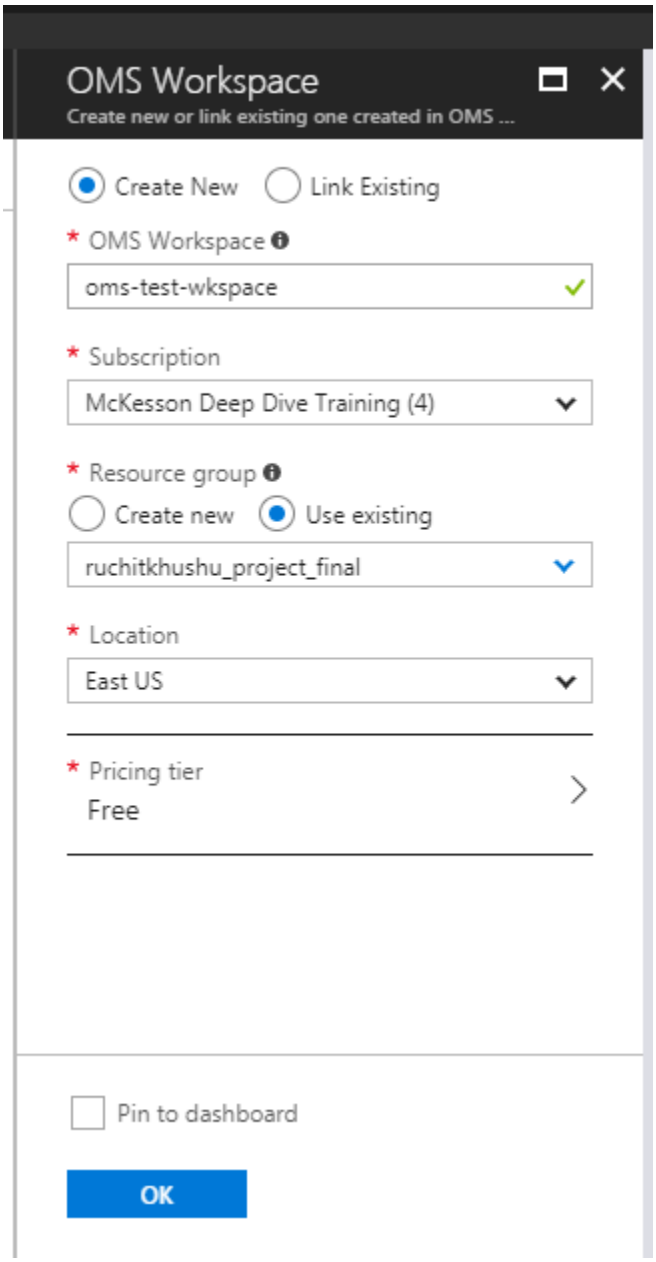


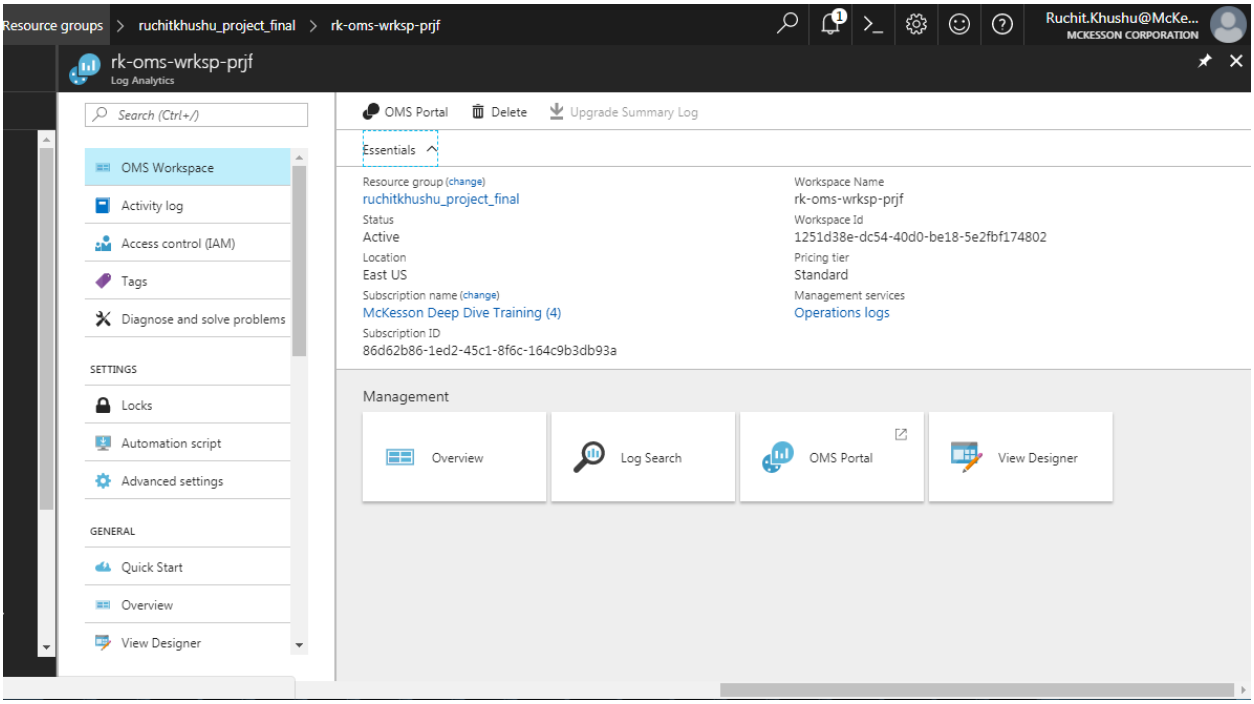
You will get the following screen listing all the workspaces for all the subscriptions and resource groups selected in the filter



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.

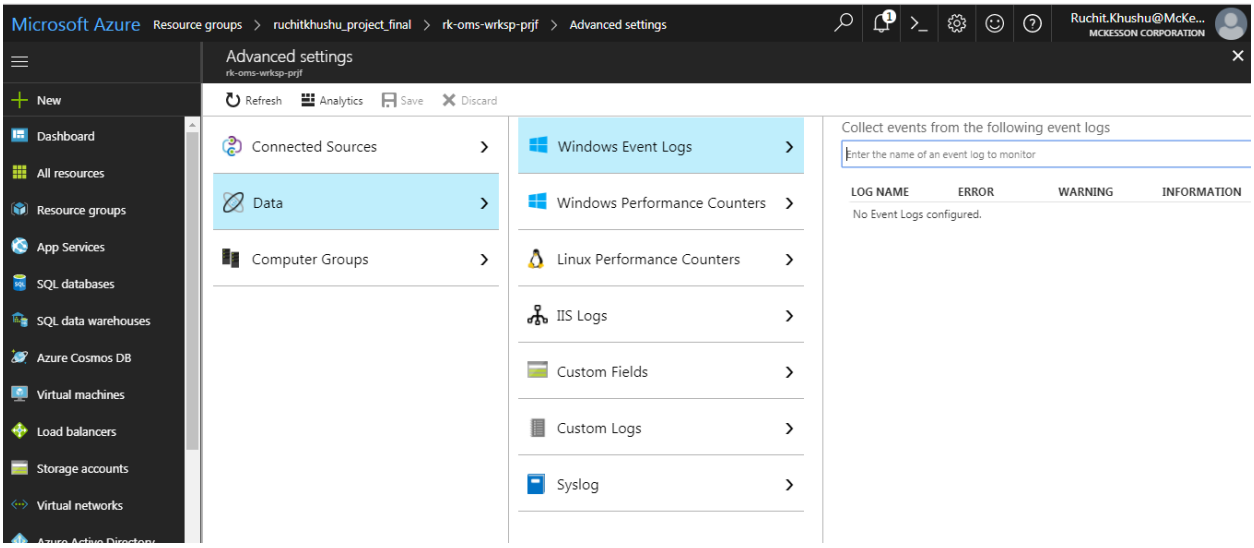


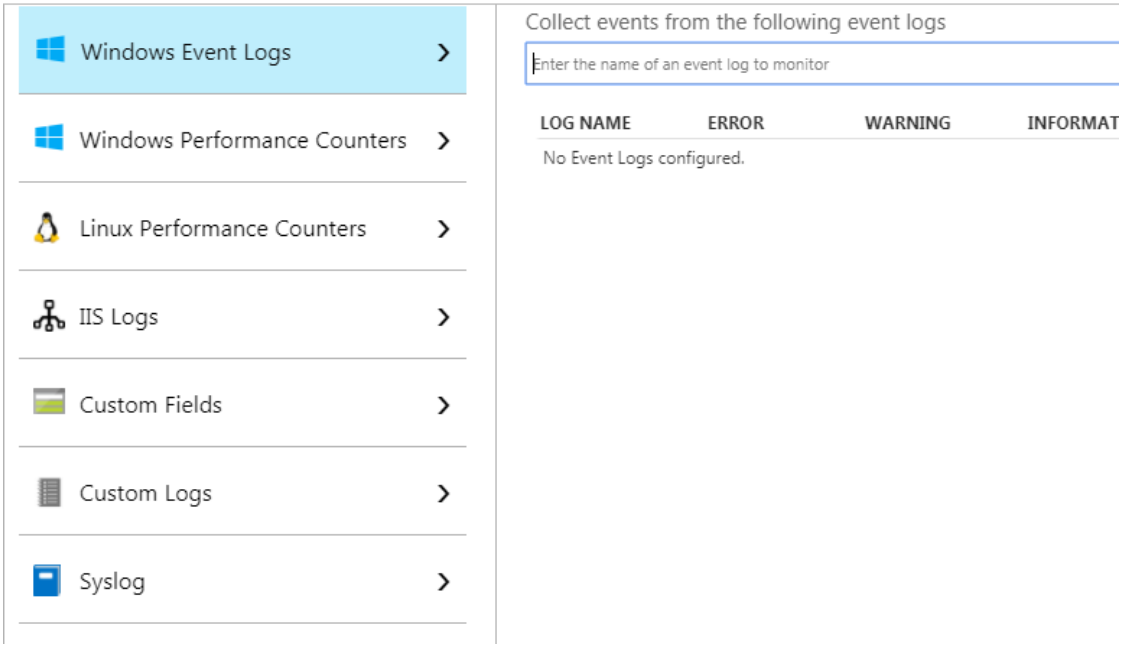


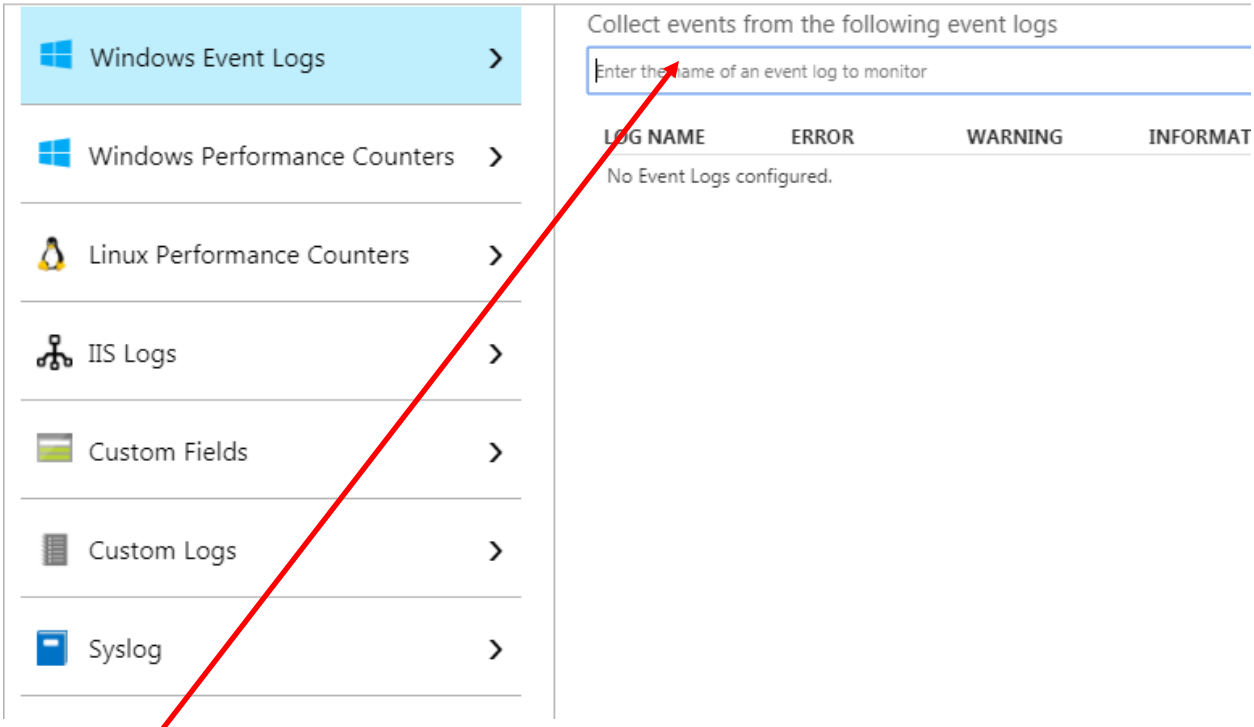
Post Creation Configuration using Azure Portal

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.

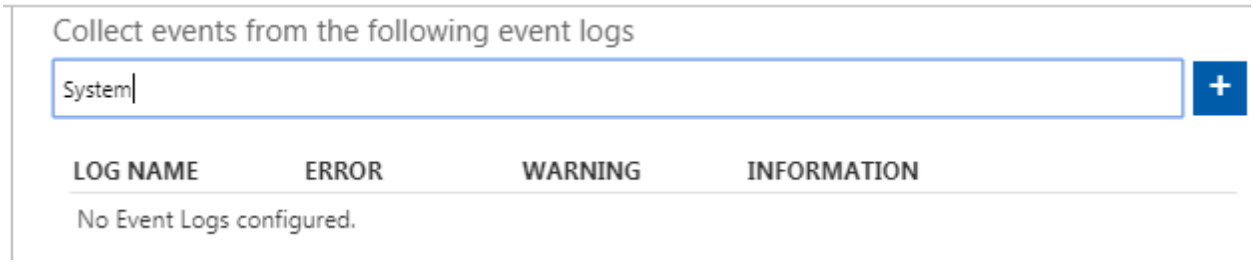
If we check the Advanced settings for OMS workspace we will see no configuration :

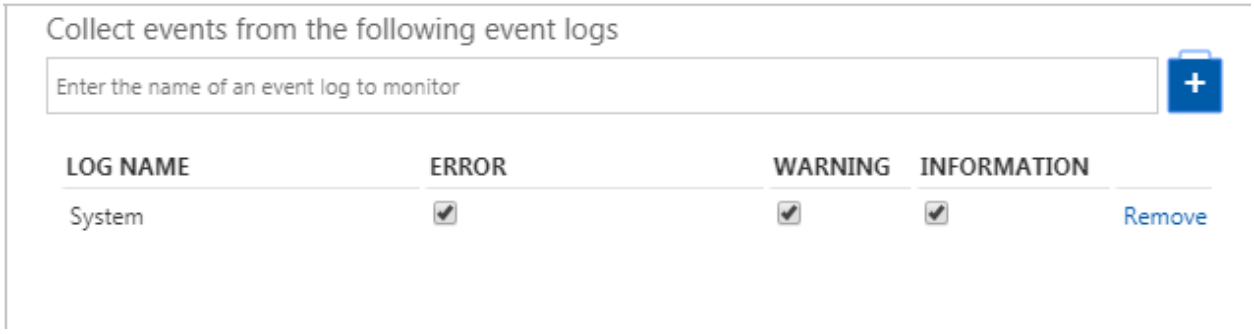




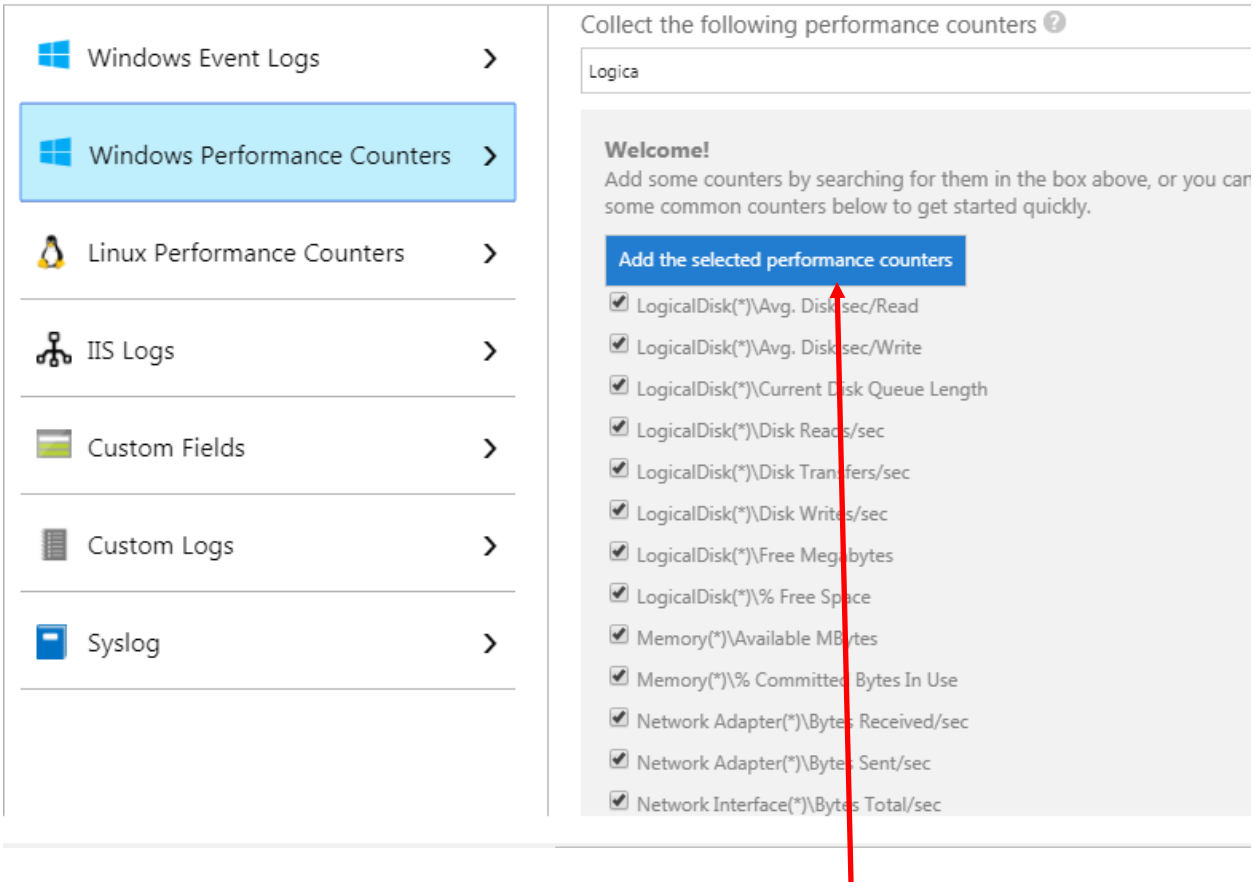


In order to add what Logs we want to monitor we should type the name of event log to be monitored in this field and press the + at the end of the field. We need to repeat this for every field we need.

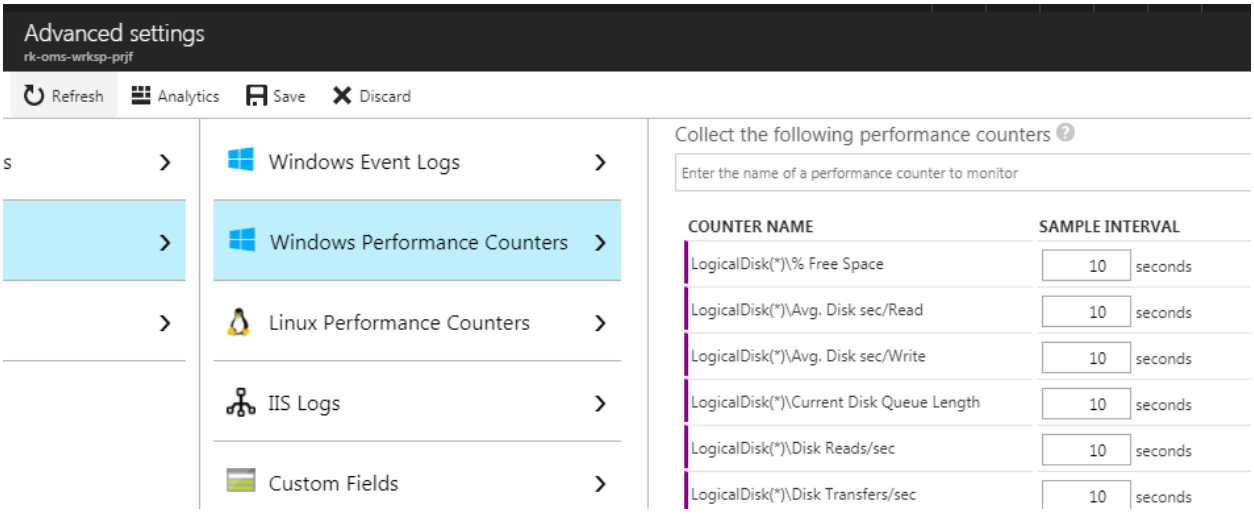




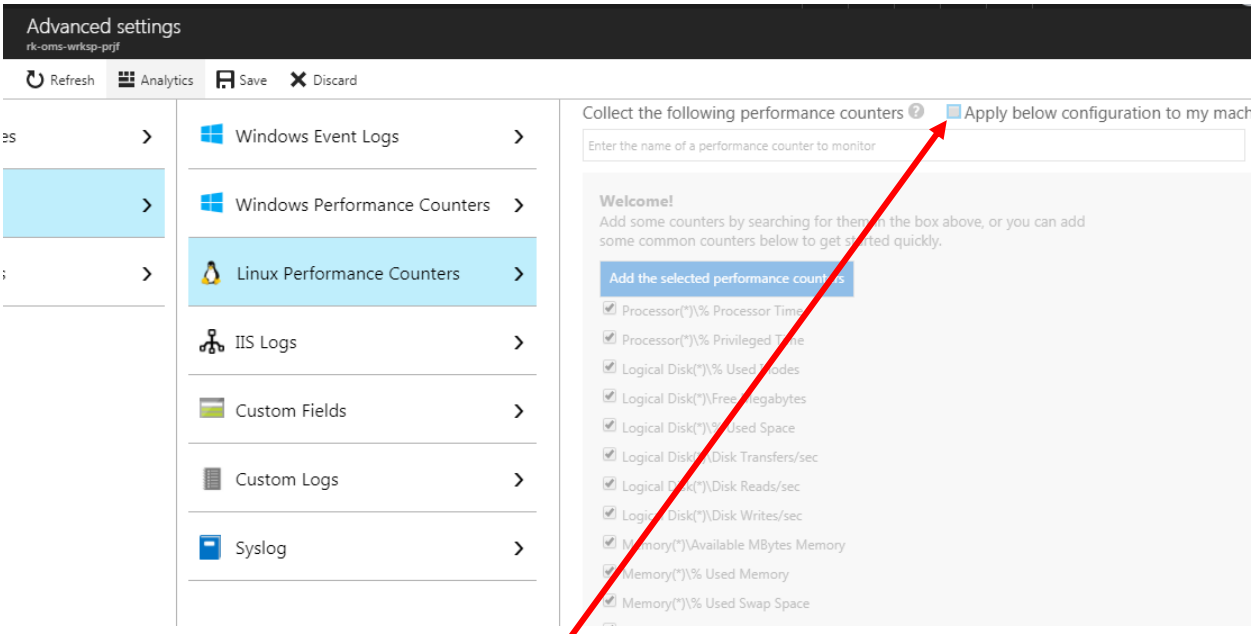
Next go to Windows Performance counter:



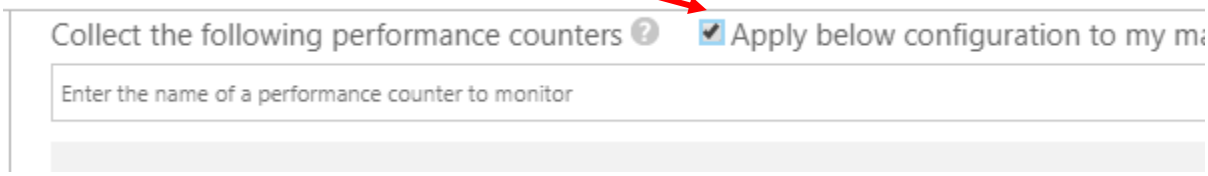
Select whatever you want to monitor and click on “Add the selected performance counters”.

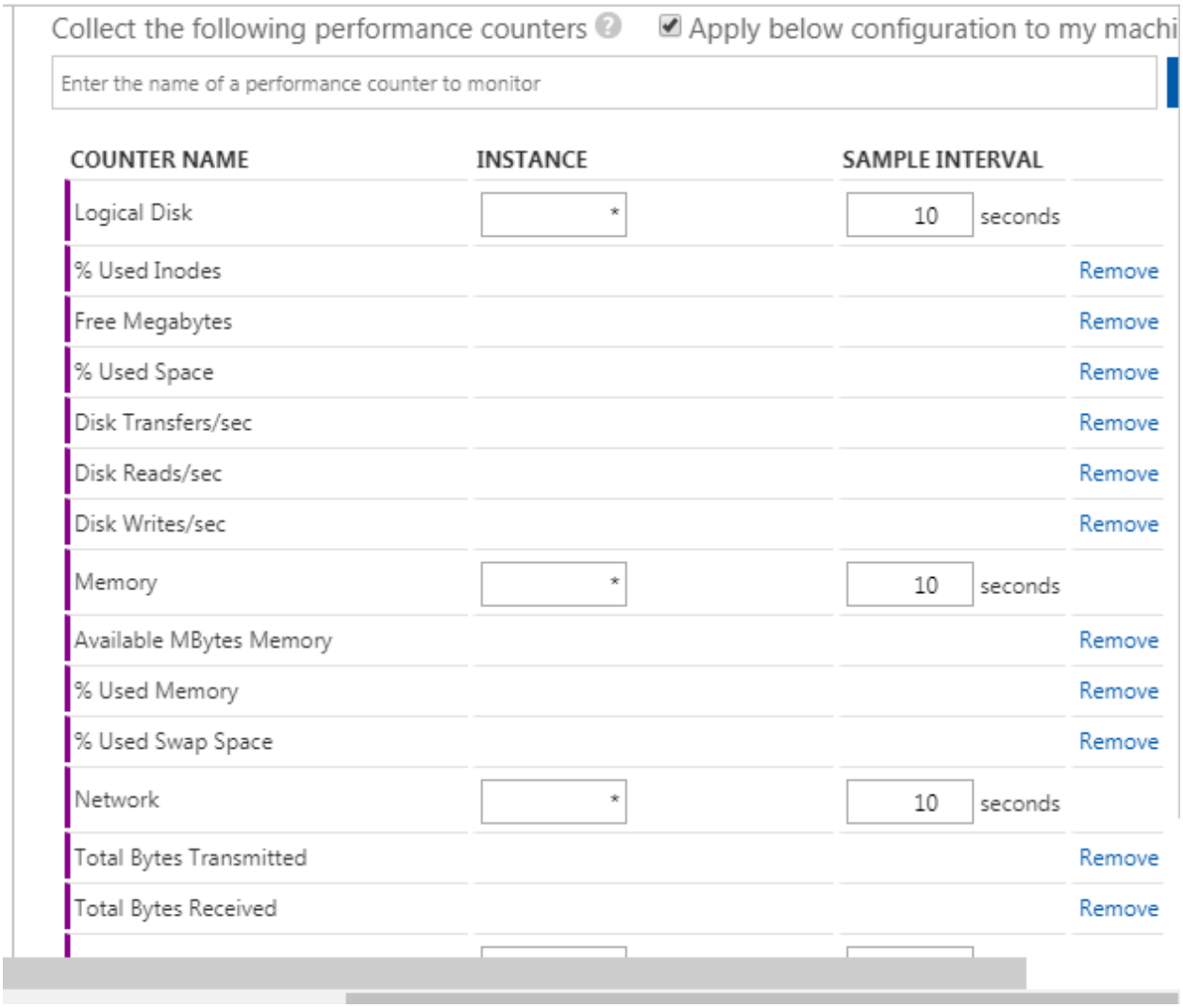


Next go to Linux Performance counters:

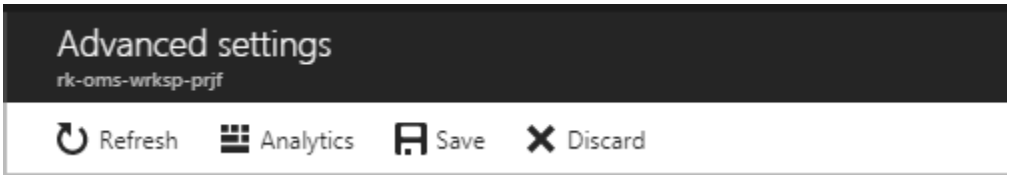


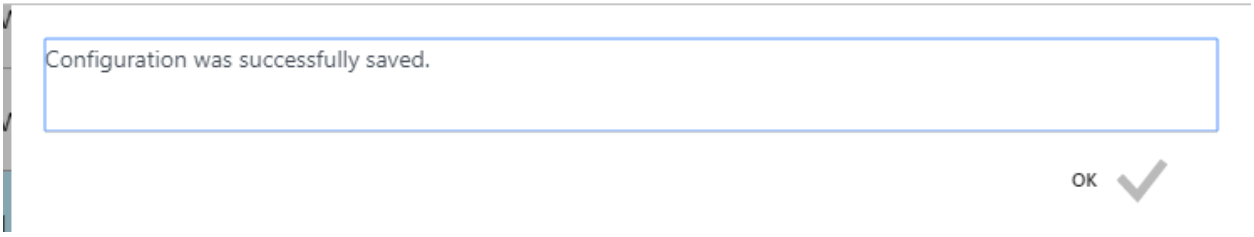
Check the checkbox on right hand top corner



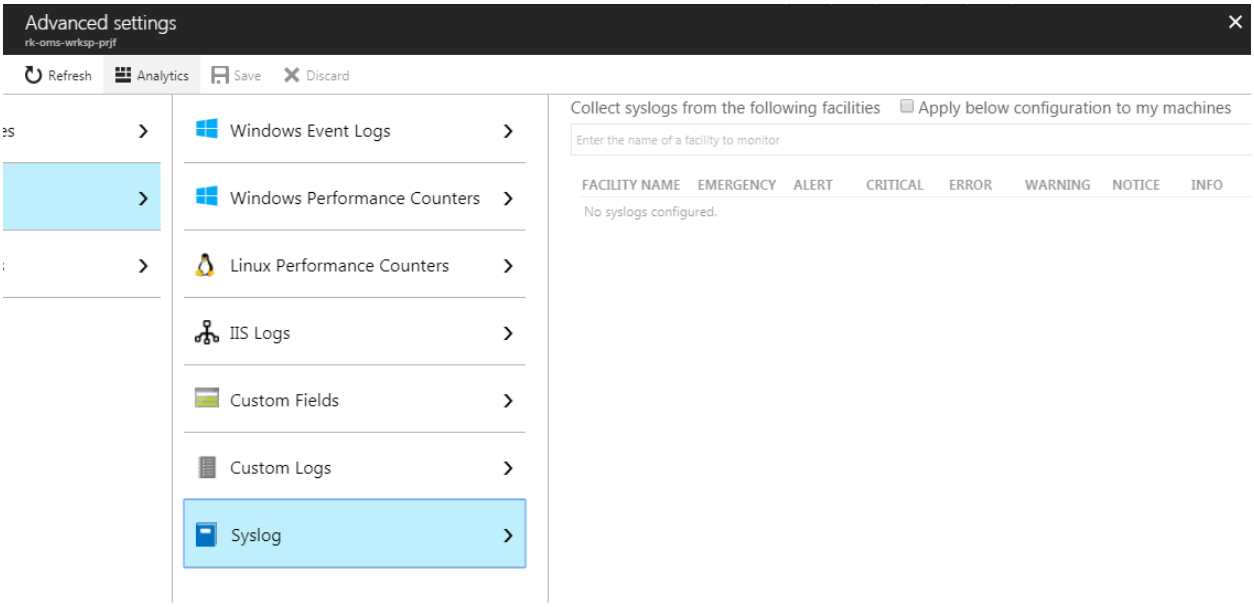


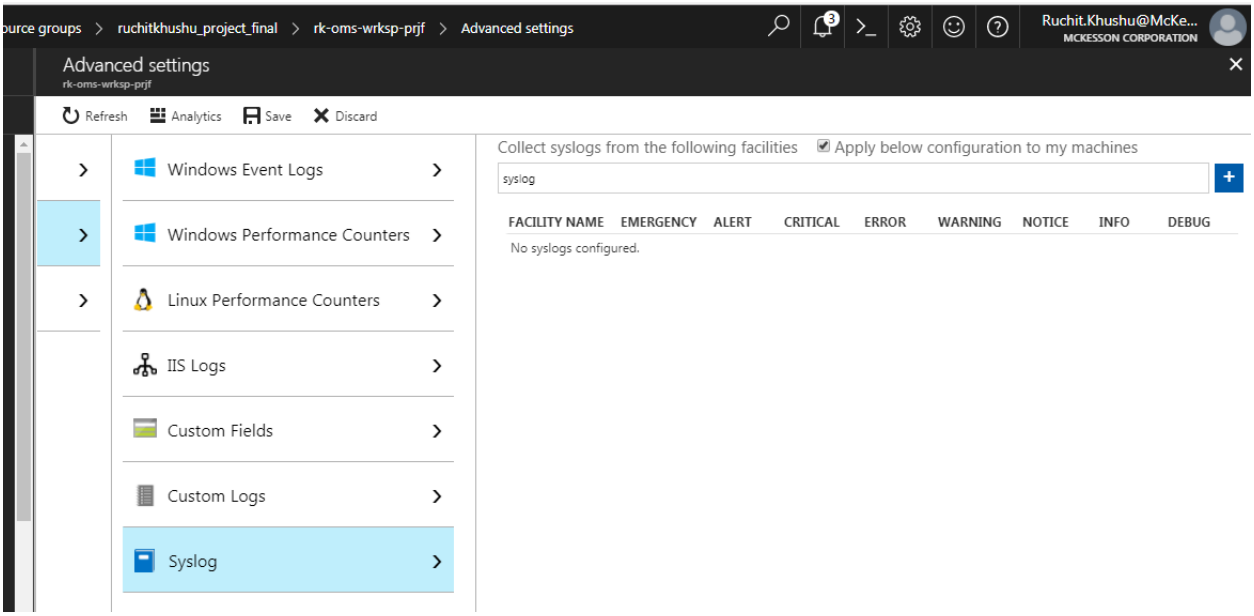
In the screen above you can make changes or go with default values. Next Save the settings

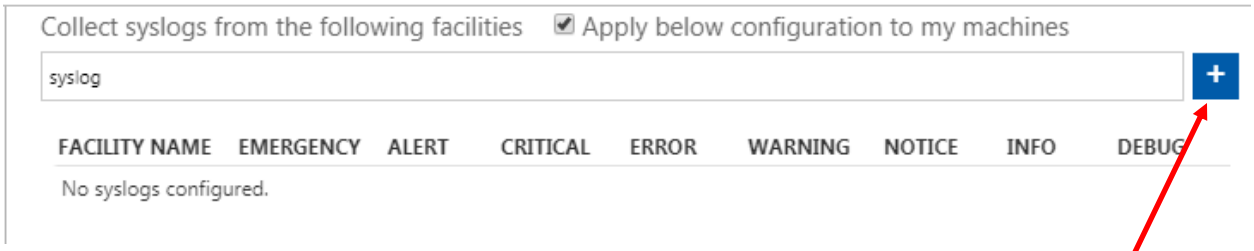




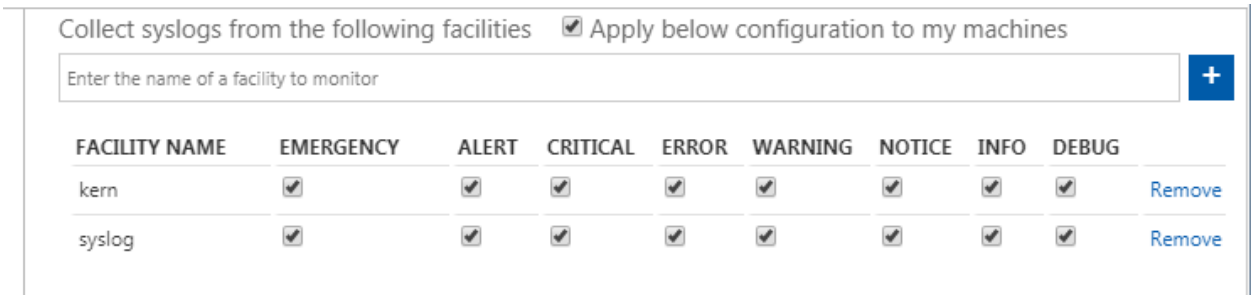
Next I configured SYSLOG:



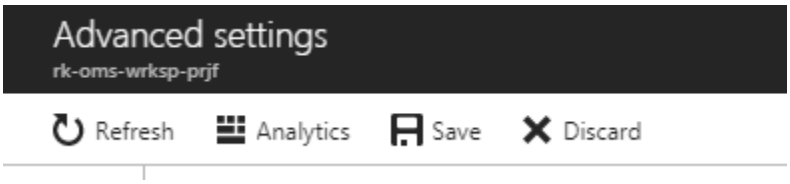




I added syslog and kern facilities.. For syslog type “syslog” in the field and then click on blue “+” button

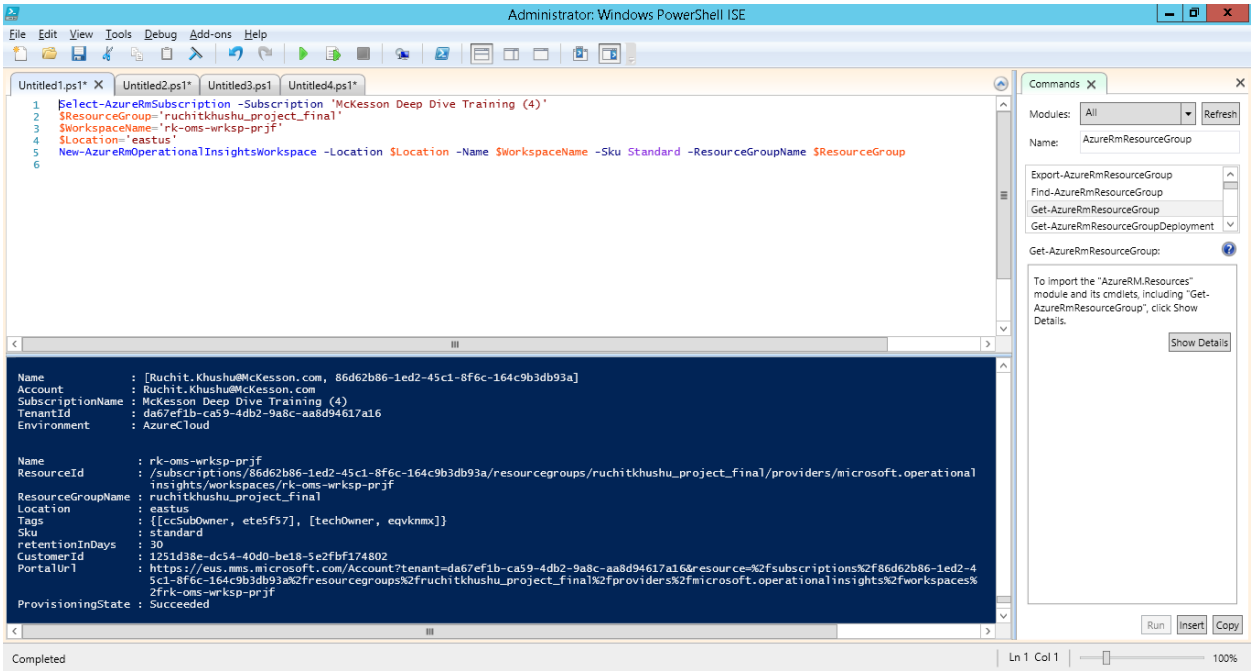


Finally save the settings.



Creating OMS Workspace Programmatically

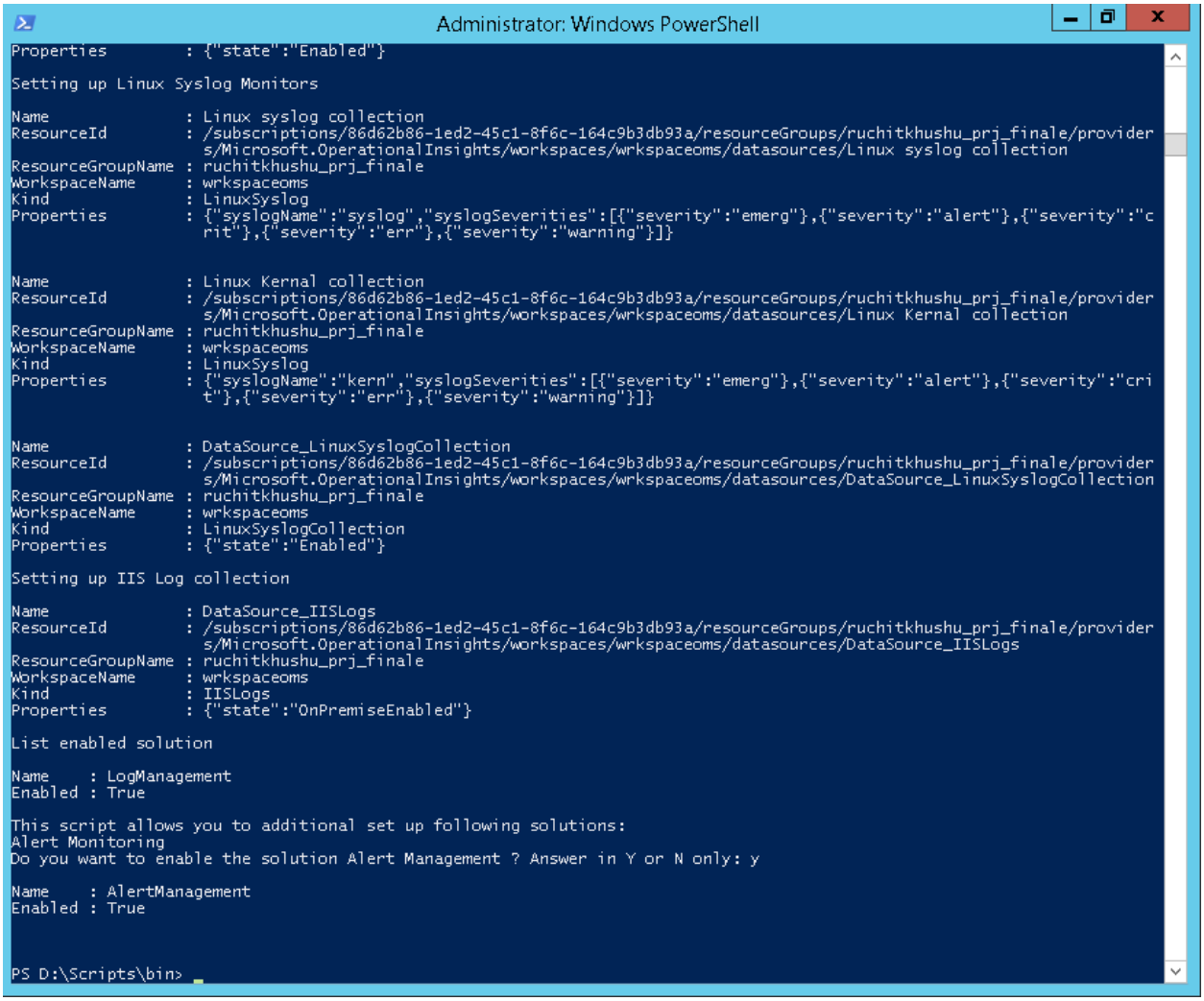
This is how we create Log Analytics Workspace Programmatically . Basically the cmdlet ***New-AzureRMOperationalInsightsWorkspace*** is used for this:



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: wrkspaceoms
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              : wrkspaceoms
ResourceId        : /subscriptions/86d62b86-1ed2-45c1-8f6c-164c9b3db93a/resourcegroups/ruchitkhushu_prj_finale/provider
                    s/microsoft.operationalinsights/workspaces/wrkspaceoms
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=%2fsubsc
                    riptions%2f86d62b86-1ed2-45c1-8f6c-164c9b3db93a%2fresourcegroups%2fruchitkhushu_prj_finale%2fprovid
                    ers%2fmicrosoft.operationalinsights%2fworkspaces%2fwrkspaceoms
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/wrkspaceoms/datasources/Example Application Event Log
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName     : wrkspaceoms
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/wrkspaceoms/datasources/System Event Log
ResourceGroupName : ruchitkhushu_prj_finale
WorkspaceName     : wrkspaceoms
Kind              : WindowsEvent
Properties        : {"eventLogName":"System","eventTypes":[{"eventType":"Error"},{"eventType":"Warning"}]}

Setting up Windows Performance Monitors
```



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 Adappter Performance Counter-2"


New-AzureRmOperationalInsightsWindowsPerformanceCounterDataSource -ResourceGroupName
$ResourceGroup -WorkspaceName $WorkspaceName -ObjectName "Network Interface" -
InstanceName "*" -CounterName ("Bytes Total/sec") -IntervalSeconds 20 -Name "Windows
Network Inteface 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", "%Priveleged 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

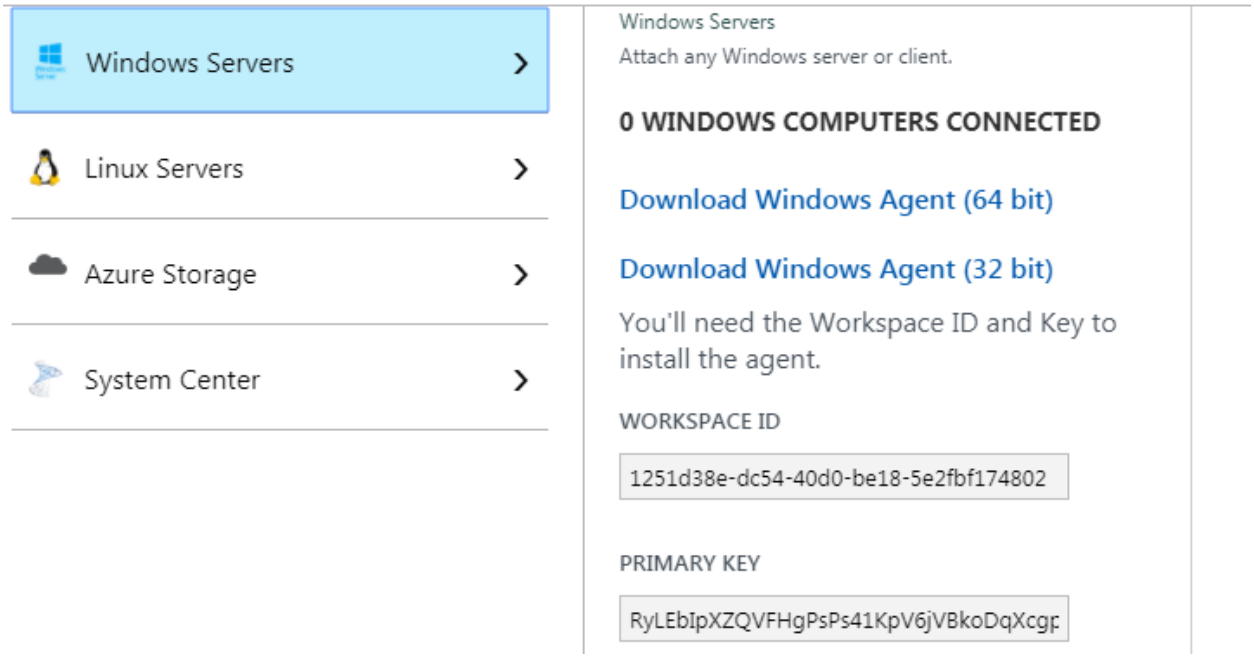
Immediately after the OMS workspace is created nothing is added to the Workspace. You can checking under Advanced Settings →Connected Systems:

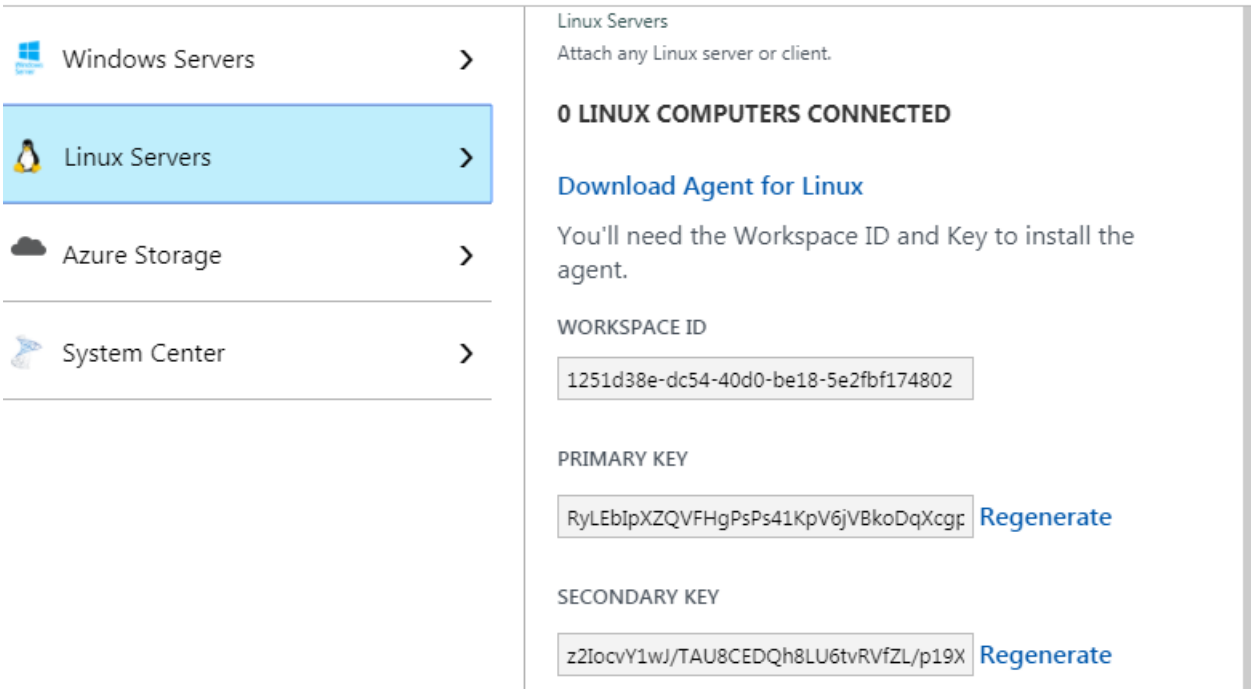
We can add following sources to OMS workspace:

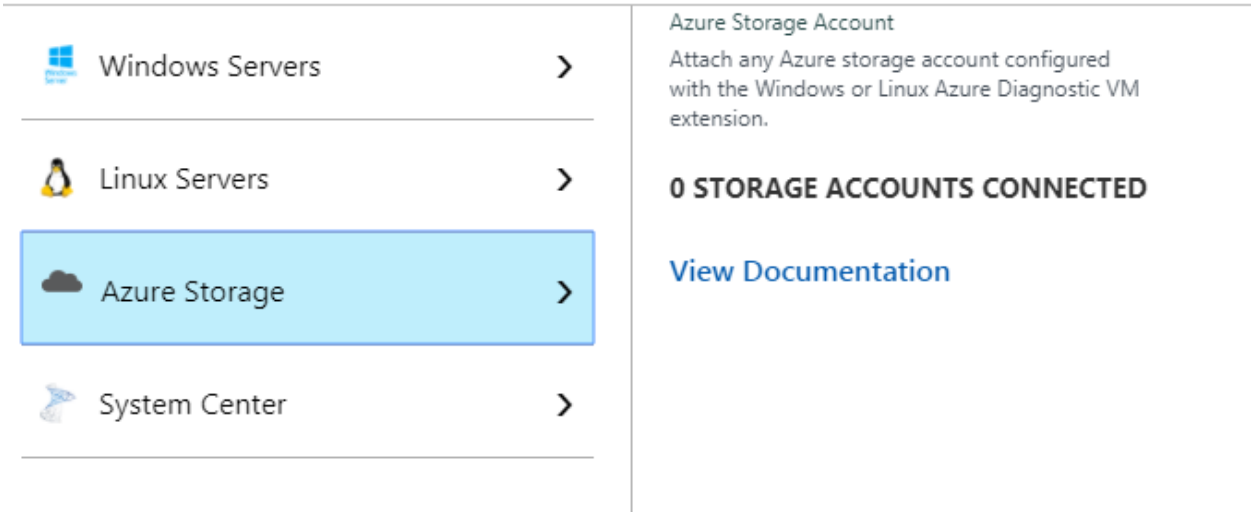
1. Azure VMs (also storage accounts)
2. On -Premise systems

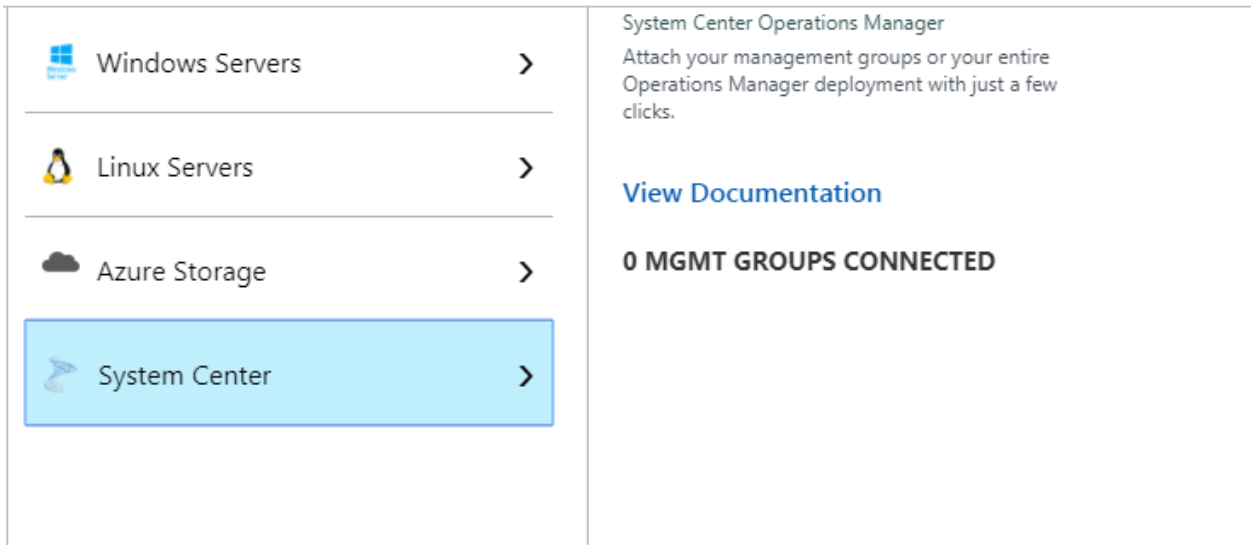
For this project we have used Azure resources only.

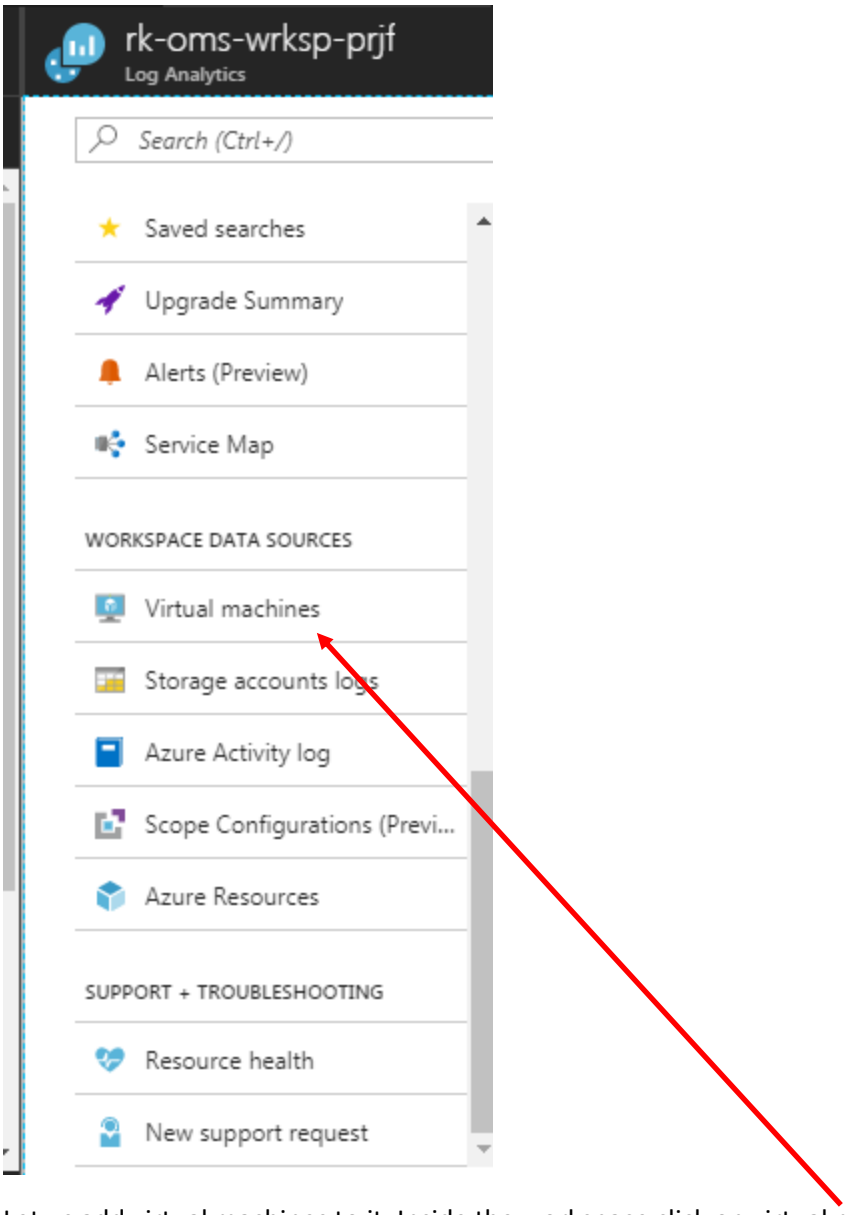
In order do so please go to section Workspace Data Sources inside the Log Analytics workspace we have created.




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
RyLEbIpXZQVFHgPsPs41KpV6jVBkoDqXcgp
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


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



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-secondry-dc	Other workspace	Windows	35c81915-5761-4cfe-b3...	SQLALWAYSONTEST01	westus
ad-secondry-dc	Other workspace	Windows	35c81915-5761-4cfe-b3...	ALWAYSONTEST01	westus
aks-nodepool1-378741...	Not connected	Linux	86d62b86-1ed2-45c1-8f...	MC_shaqs-rg_shaqsAKS...	eastus
aks-nodepool1-378741...	Not connected	Linux	86d62b86-1ed2-45c1-8f...	MC_shaqs-rg_shaqsAKS...	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

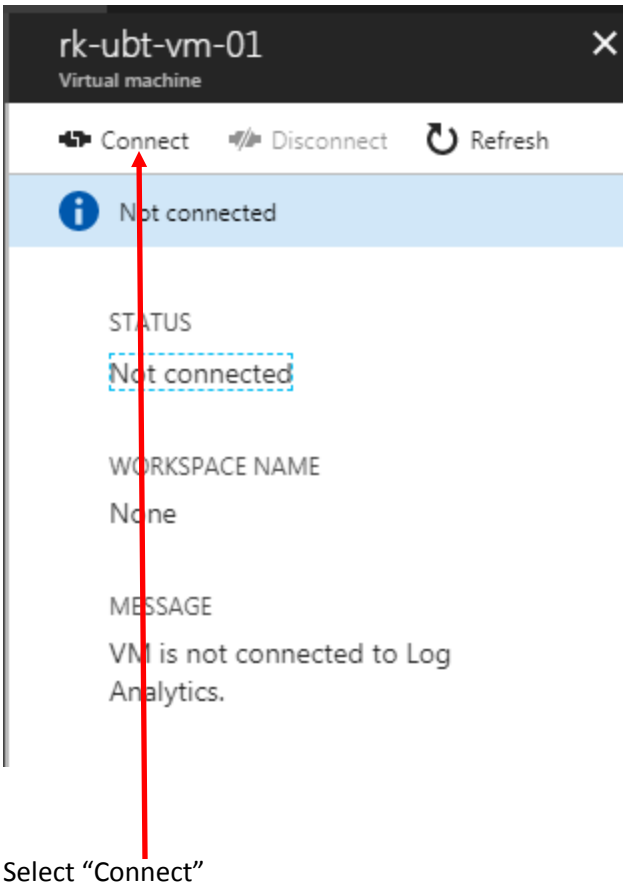
You need to select the VM you want to add to the workspace. Please note 1 VM can be added to 1 Workspace at any given point of time.. We can manually filter by Virtual machine name or broader criteria like Subscription name, Resource group name etc.

Refresh Help

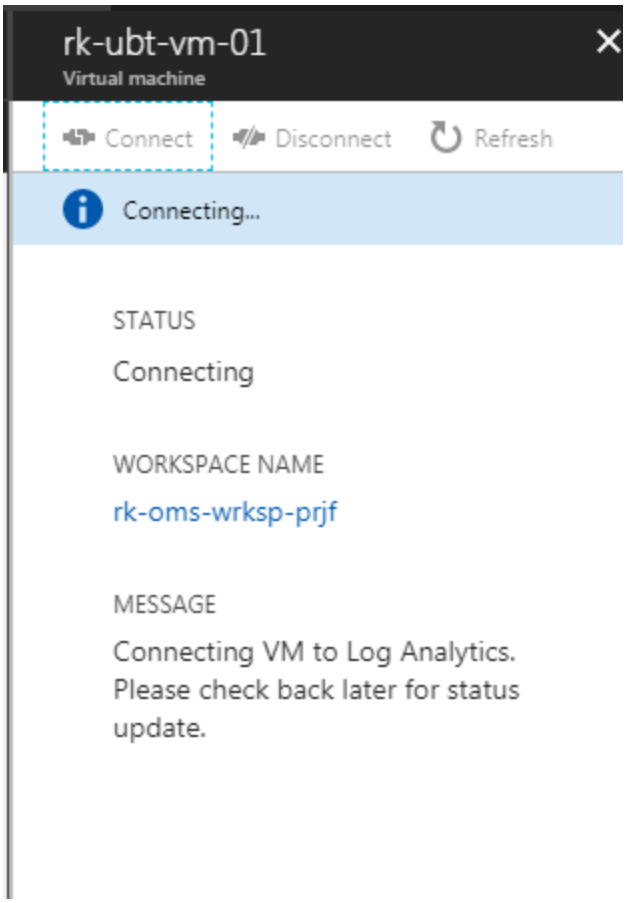
Filter by name... | 8 selected | 2 selected | McKesson Deep Div... | ruchitkhushu_projec... | 5 selected

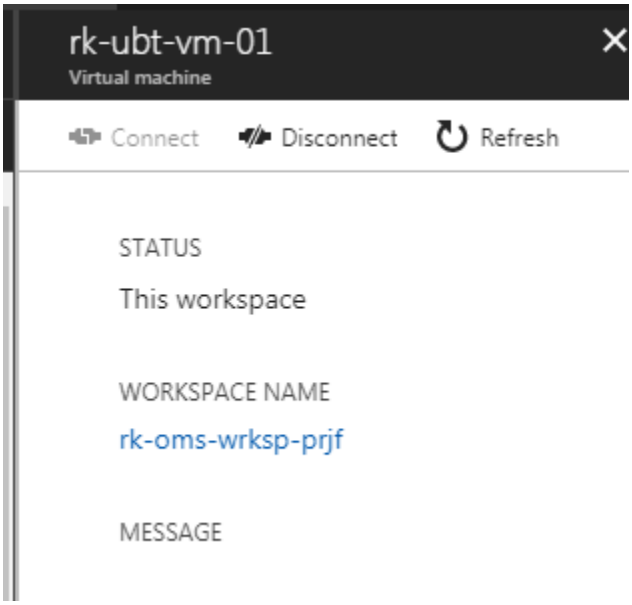
NAME	OMS CONNECTION	OS	SUBSCRIPTION	RESOURCE GROUP	LOCATION
rk-ubt-vm-01	Not connected	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
rk-ubt-vm-02	Not connected	Linux	86d62b86-1ed2-45c1-8f...	ruchitkhushu_project_final	westus
rk-win-vm-01	Not connected	Windows	86d62b86-1ed2-45c1-8f...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

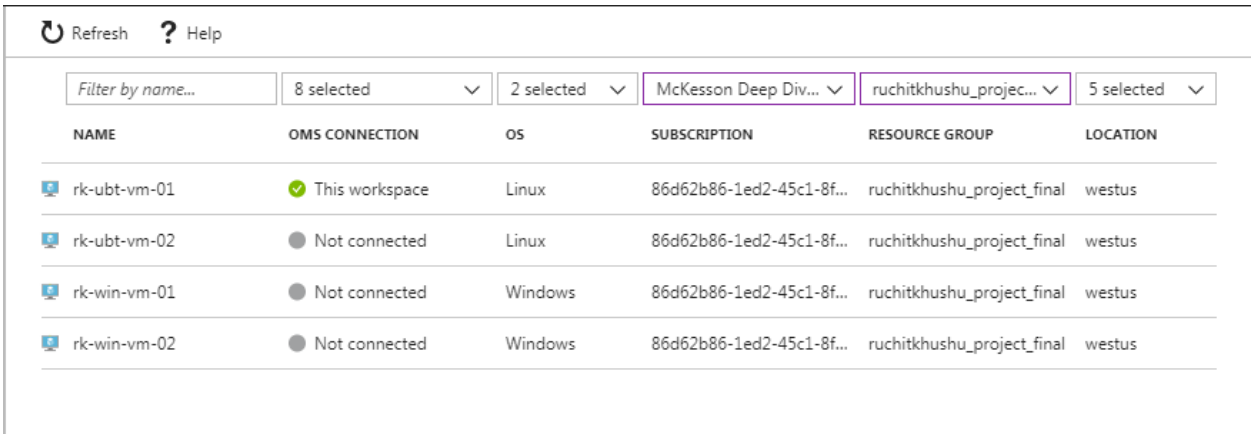
Click on the VM and connect to OMS



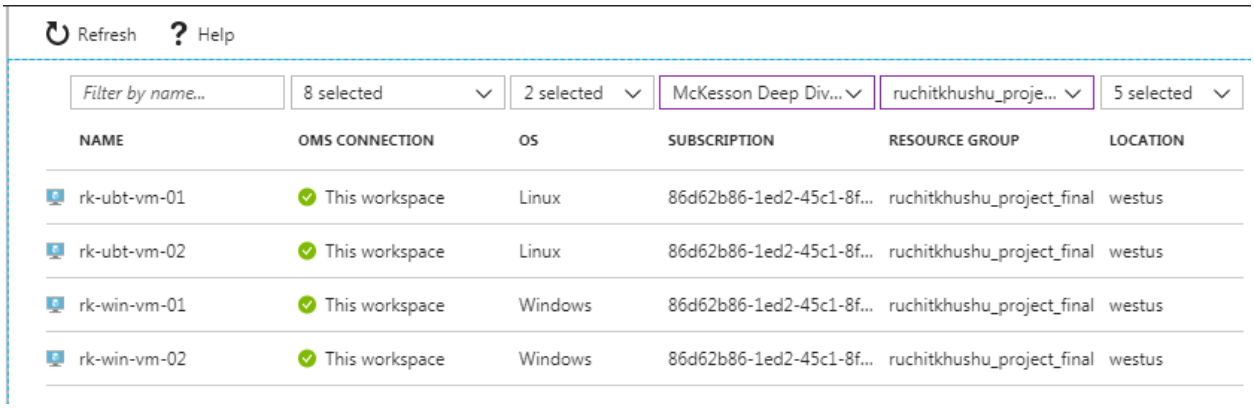
Select “Connect”


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.

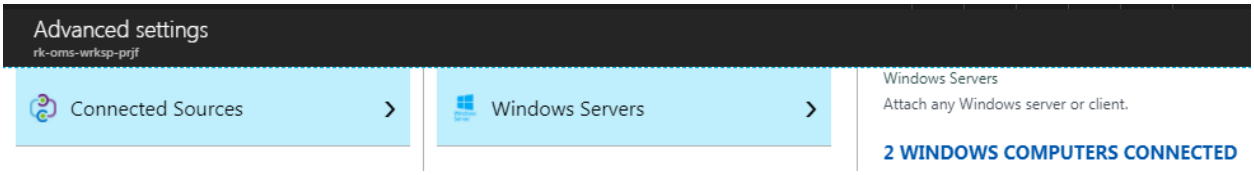

rk-ubt-vm-01
Virtual machine
Connect
Disconnect
Refresh
STATUS
This workspace
WORKSPACE NAME
rk-oms-wrksp-prjf
MESSAGE

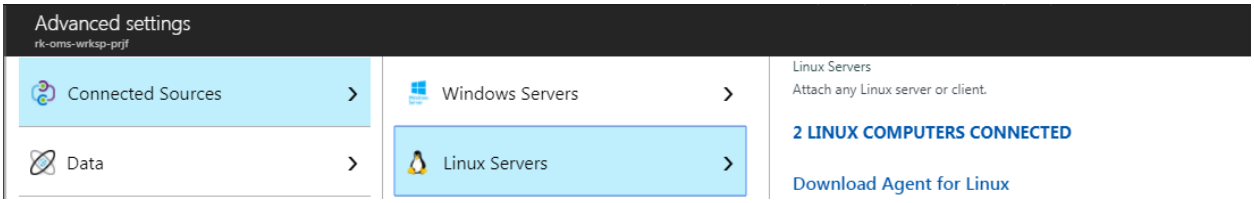


Do it for all the VMs that need to be connected…



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





Adding Resources to Log Analytics Workspace Programmatically

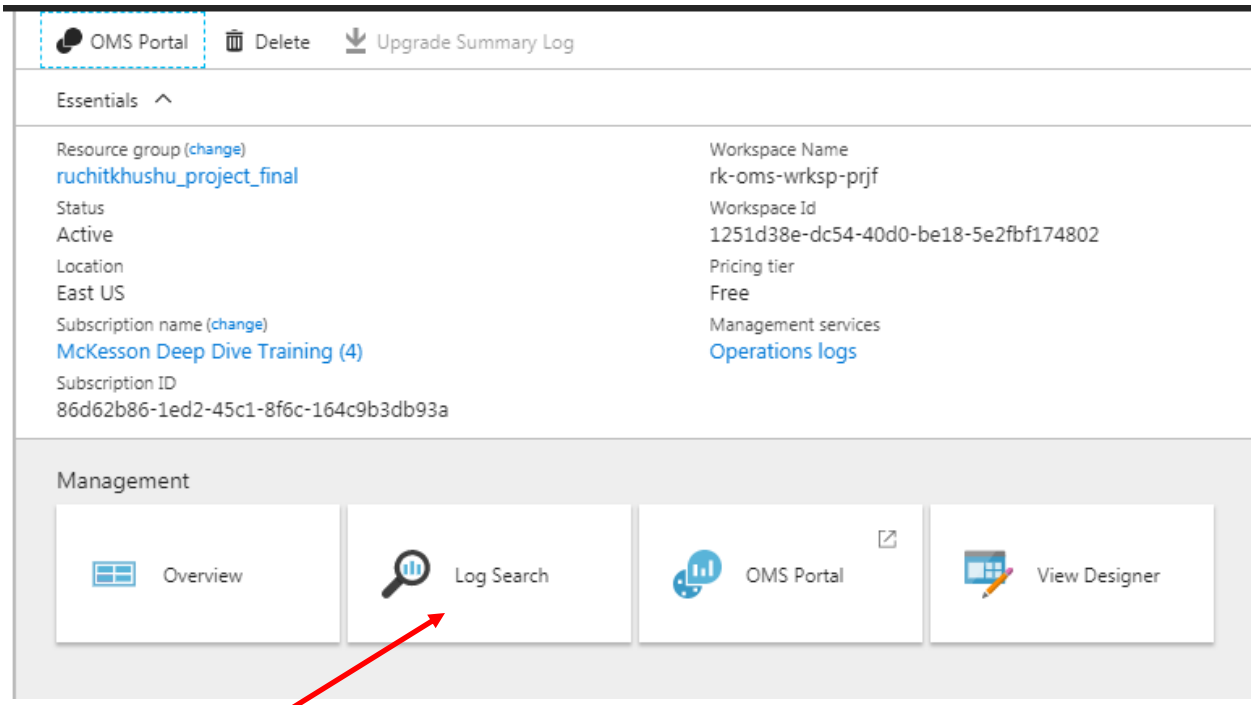
Adding VM one by one to Azure Portal can be cumbersome if there are two many VMs. So we can do it programmatically using PowerShell

I have created a simple script that add 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 :**OMSaddresournce.ps1**

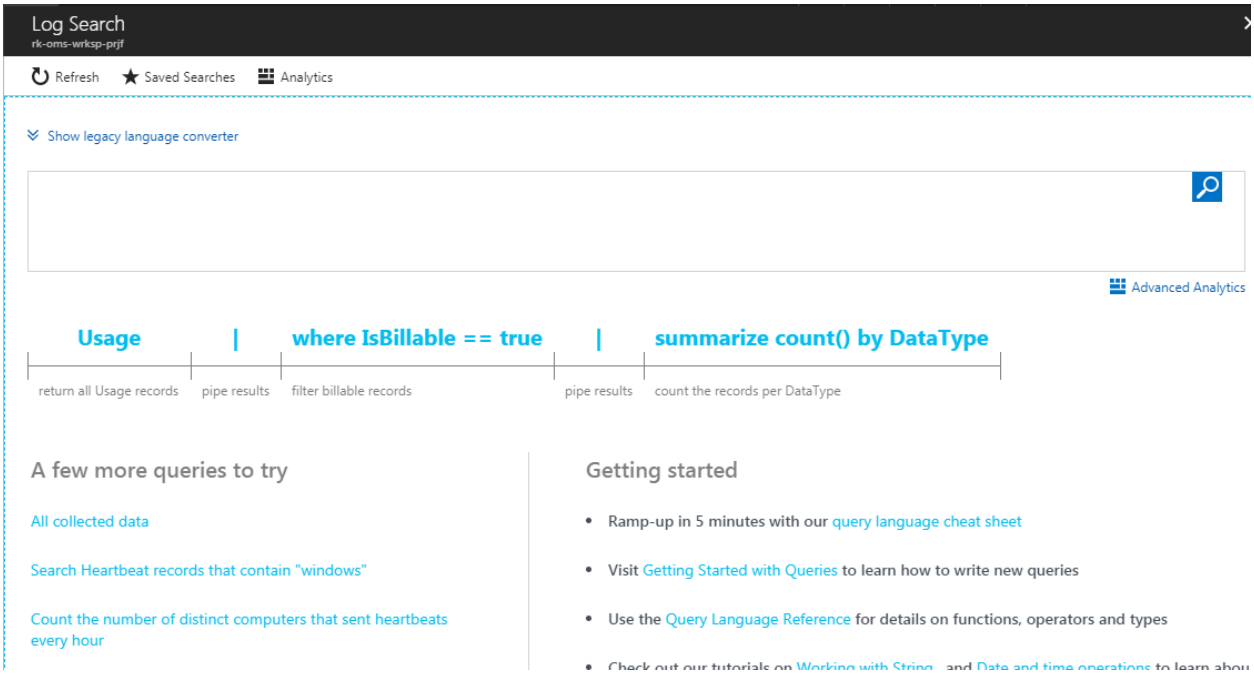
```
$subscriptionid=Read-Host 'Input the subscription ID:'

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 Configring the OMS Key.'

Import-CSV $file | ForEach-Object {

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

Write-Host "Installing and Configring 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"
  }


}
```

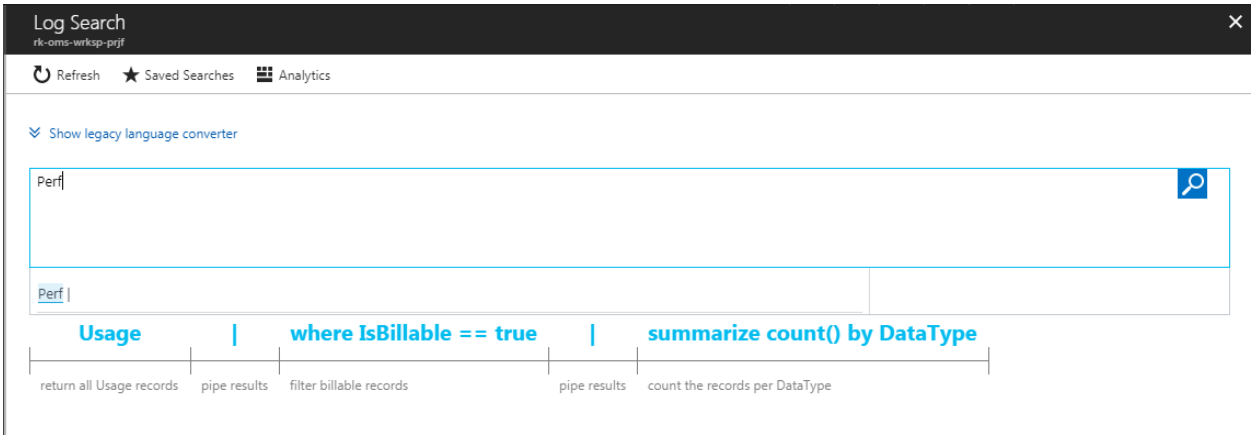
Log Search

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

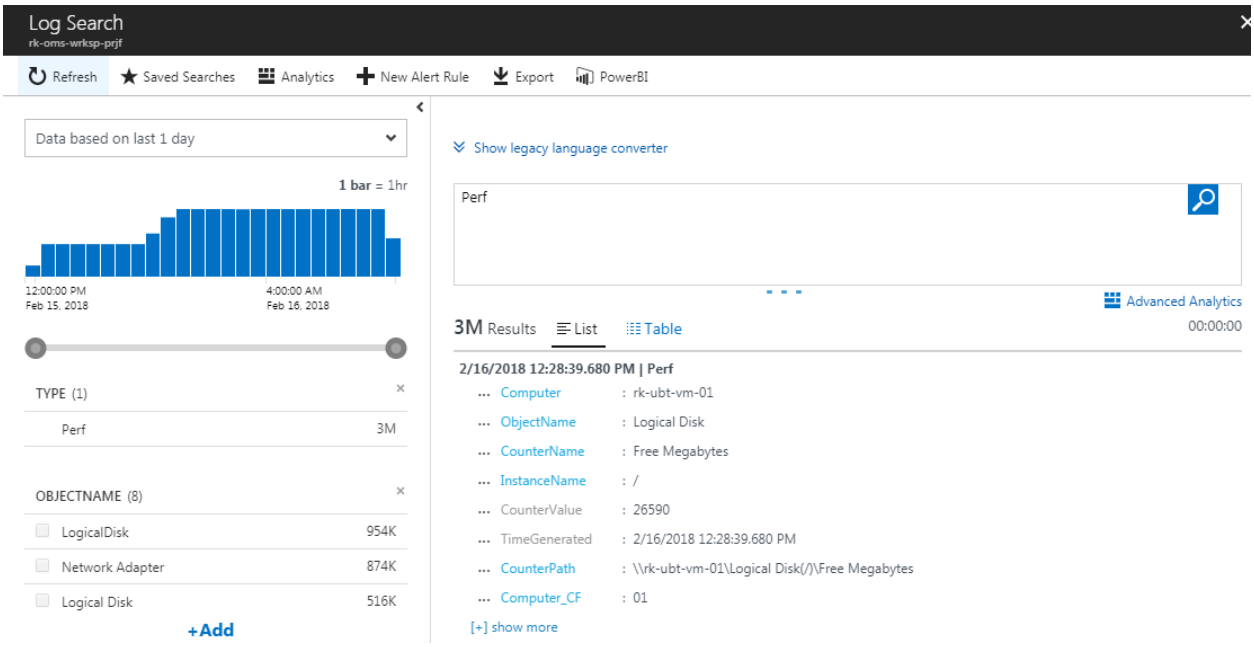


Click on Log search





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



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) ×

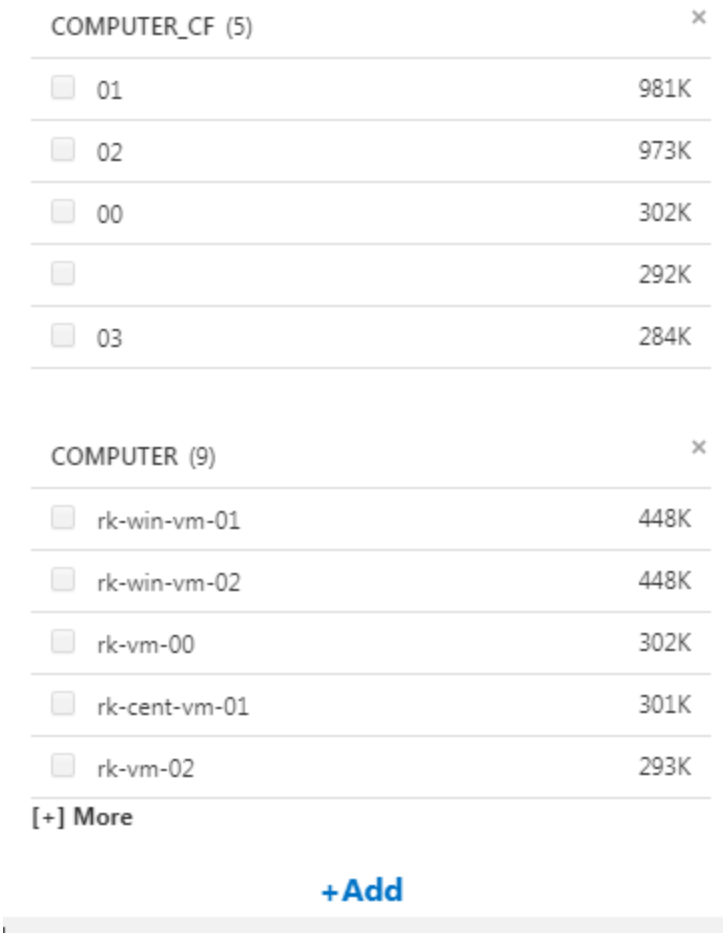
LogicalDisk	954K
Network Adapter	874K
Logical Disk	516K
Processor	160K
Memory	157K

[+] More

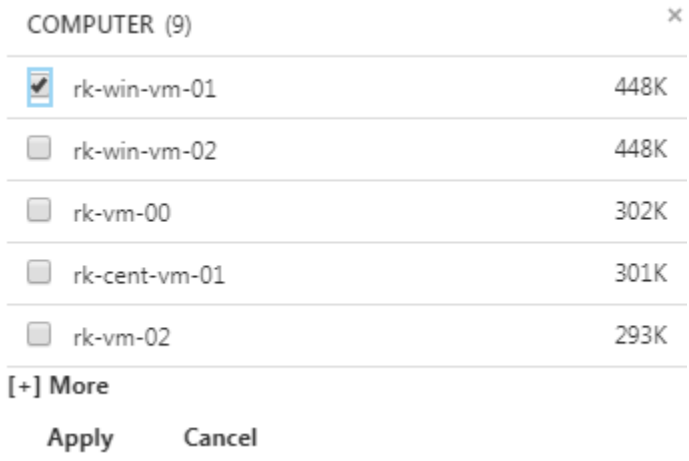
COUNTERNAME (23) ×

Bytes Received/sec	437K
Bytes Sent/sec	437K
Disk Writes/sec	205K
Free Megabytes	205K
Disk Transfers/sec	205K

+Add



We can add filters to this query by selecting the dimensions



Show legacy language converter

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

Advanced Analy

449K Results List Table 00:00:0

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 12:28:09.060 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

1 bar = 1hr

12:00:00 PM Feb 15, 2018 — 4:00:00 AM Feb 16, 2018

TYPE (1)

Perf 9K

OBJECTNAME (1)

System 9K

COUNTERNAME (1)

+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

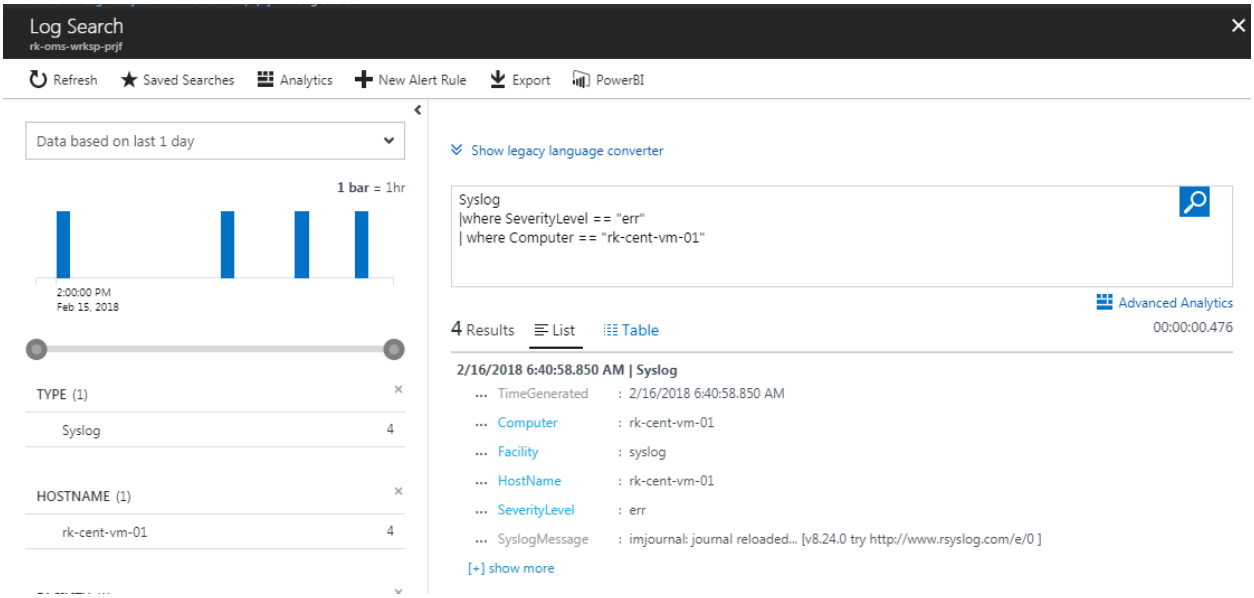
TimeGenerated	Computer	CounterName	Computer_CF	Counter
2/16/2018 12:28:09.060 PM	rk-win-vm-01	Processor Queue Length	01	0
2/16/2018 12:28:19.103 PM	rk-win-vm-01	Processor Queue Length	01	0
2/16/2018 12:28:29.117 PM	rk-win-vm-01	Processor Queue Length	01	0
2/16/2018 12:28:39.137 PM	rk-win-vm-01	Processor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

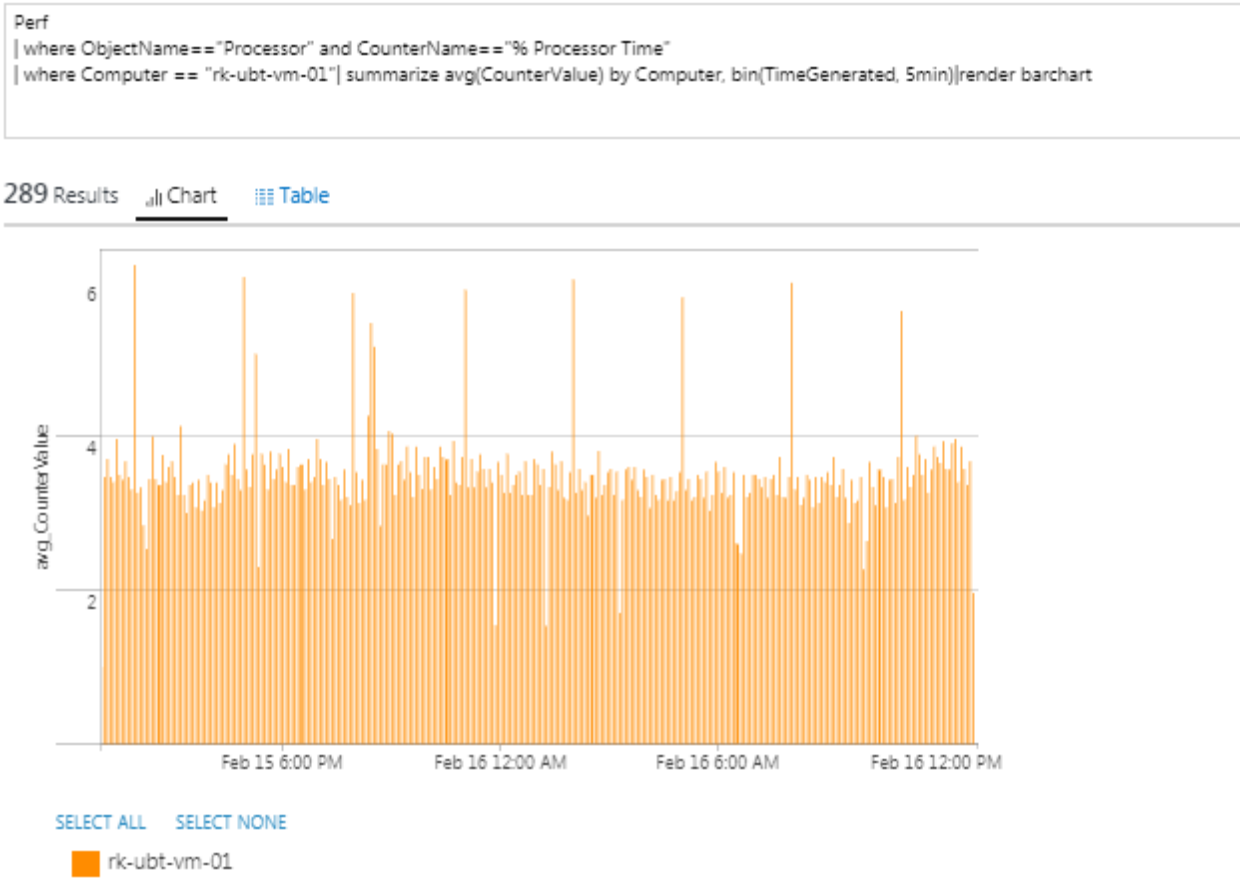


Here is how processor time looks like

Perf

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

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

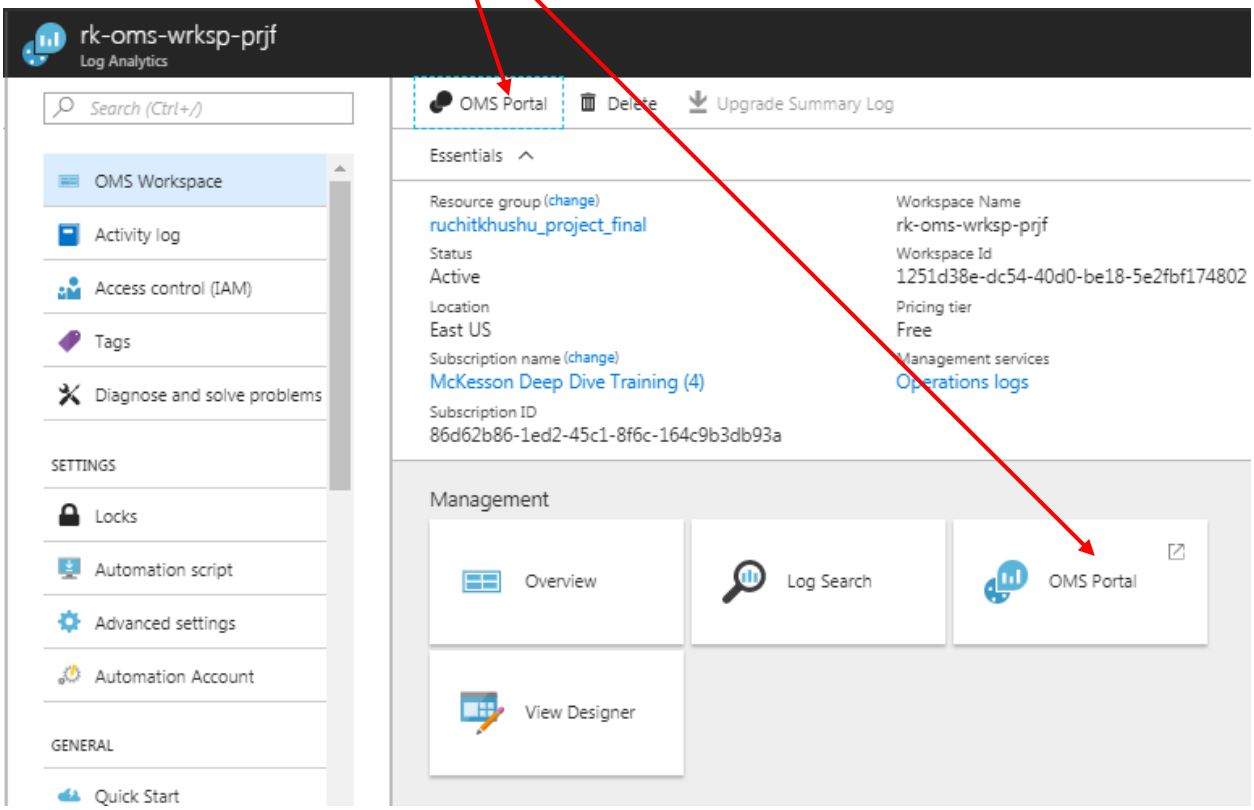


Next we will create some alerts and dashboard

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

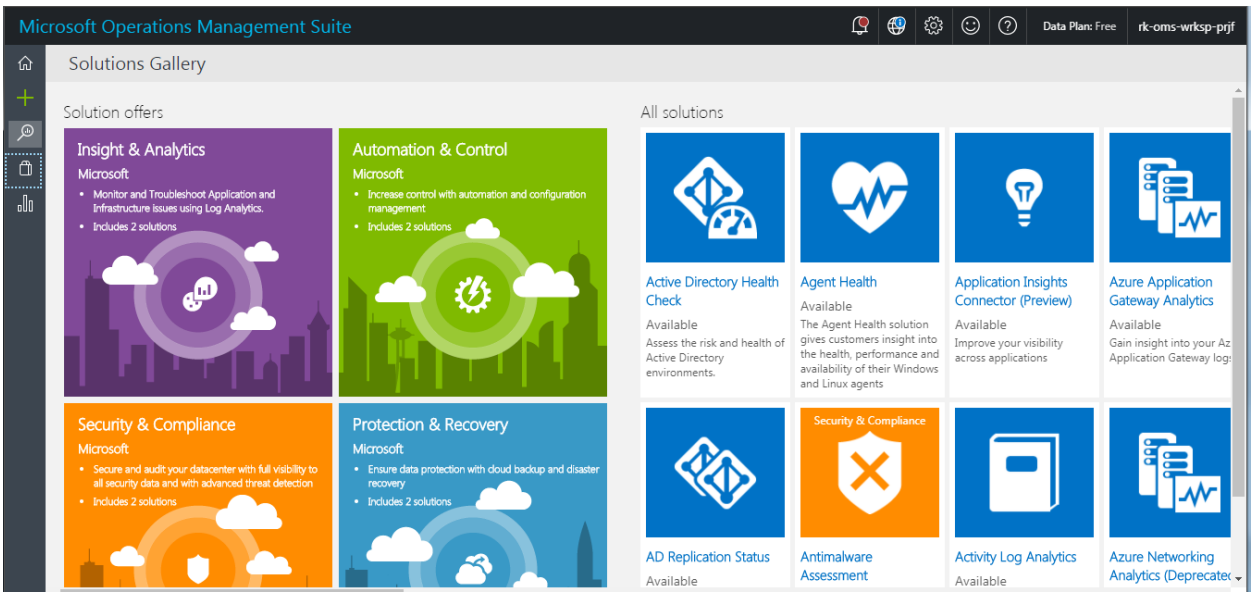
We can go from Overview to OMS Portal



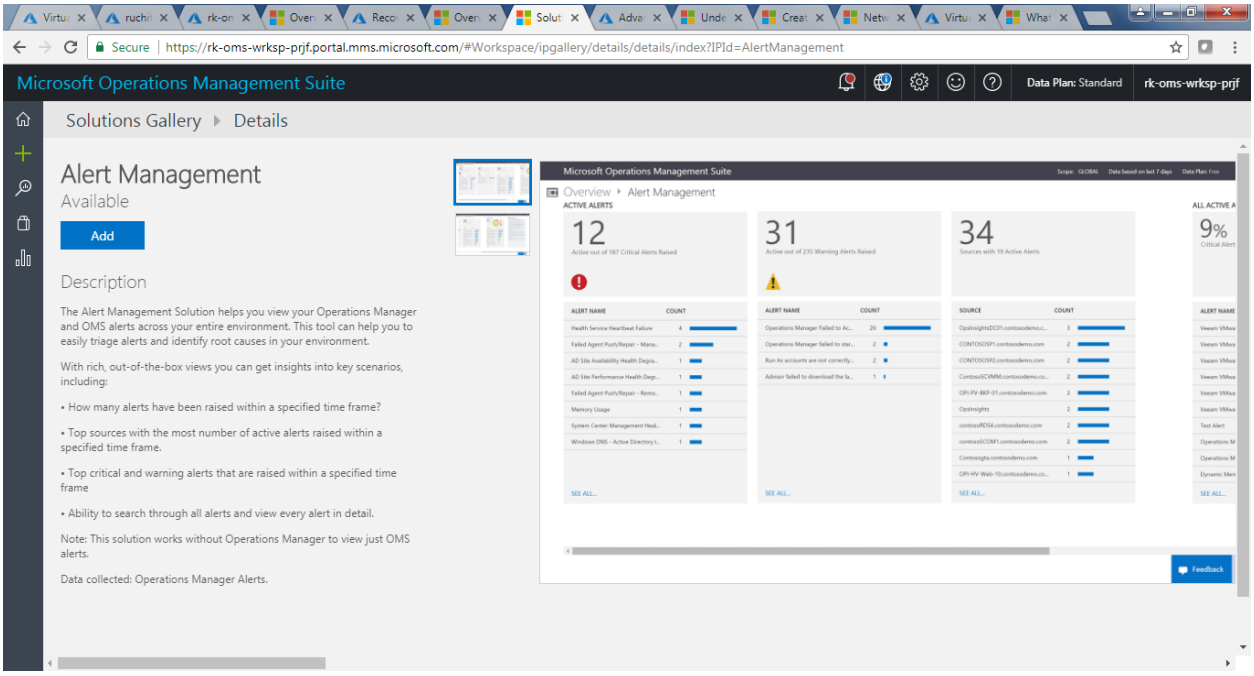
OMS portal url is : https://<OMS-workspacename>.portal.mms.microsoft.com/

Add Solutions using OMS Portal

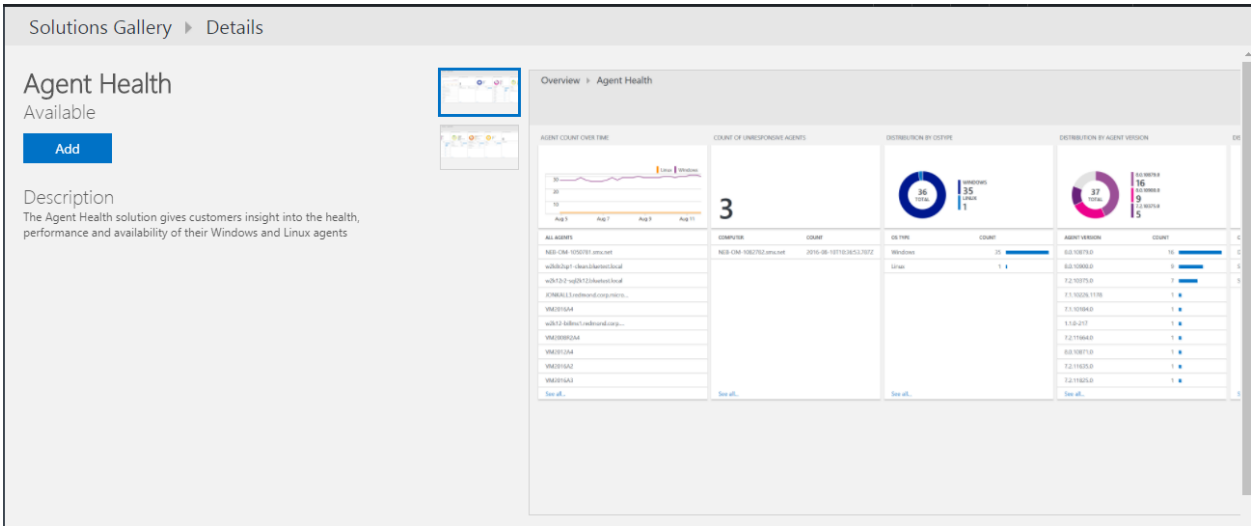
Inside the OMS portal you can choose ready to be deployed solution from Solution Gallery



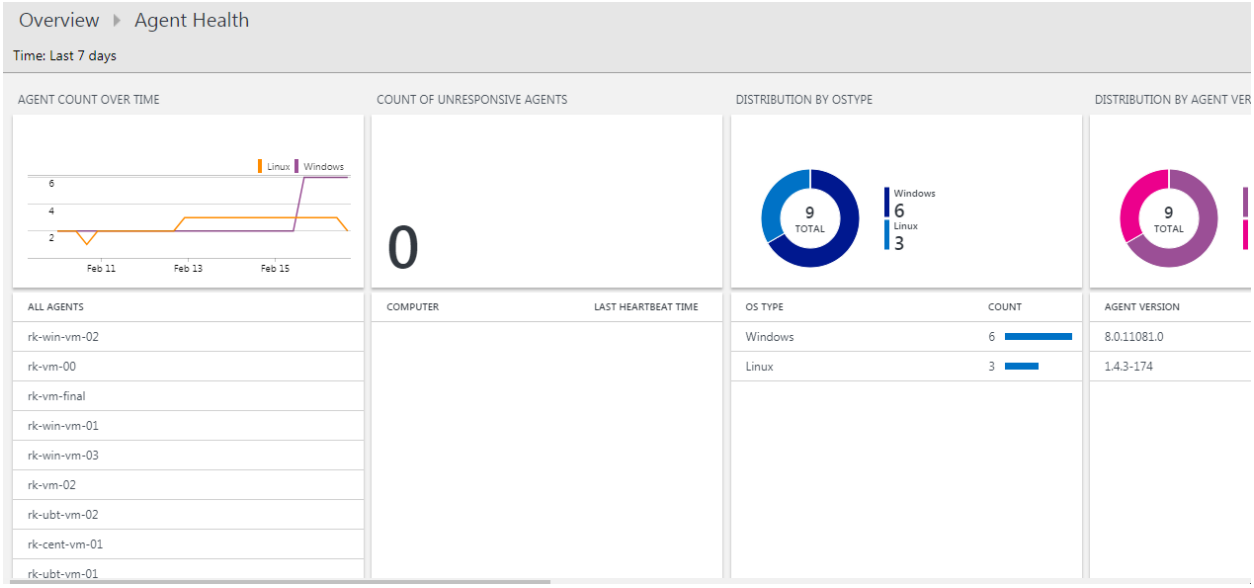
I deployed Alert Monitoring and Change Management manually . To deploy any solution we have double click on it and follow the instructions .



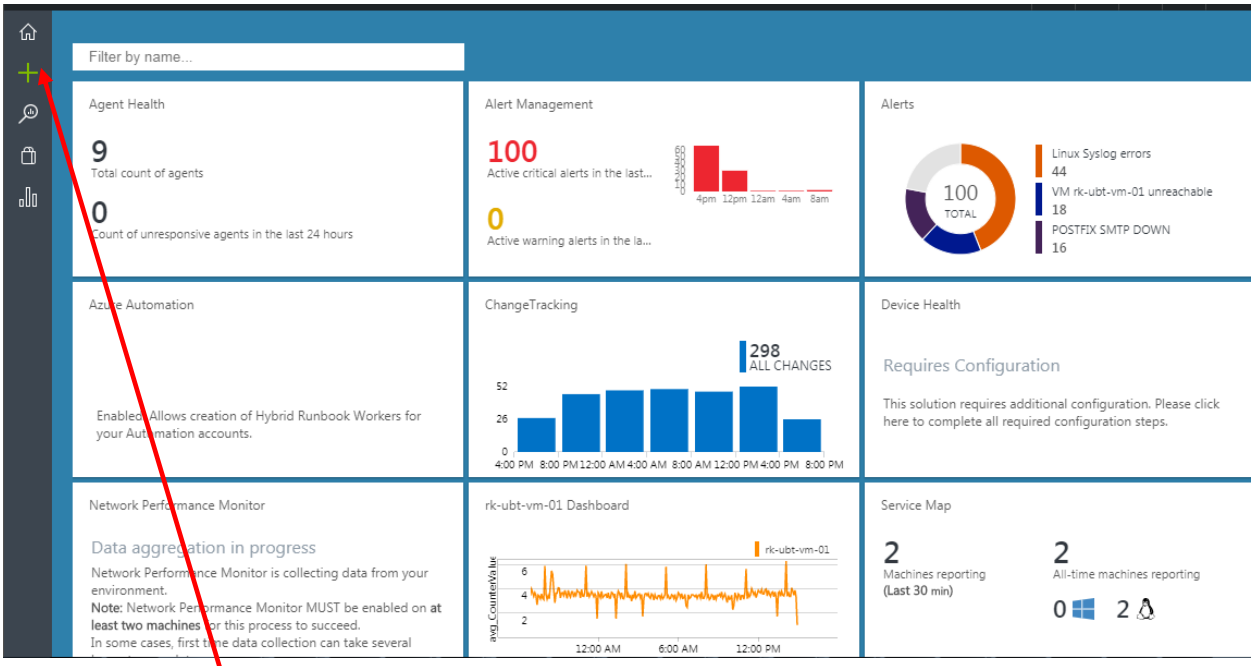
Here is example of how to add one of solutions: Agent Health



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



Create custom Dashboards in OMS Portal

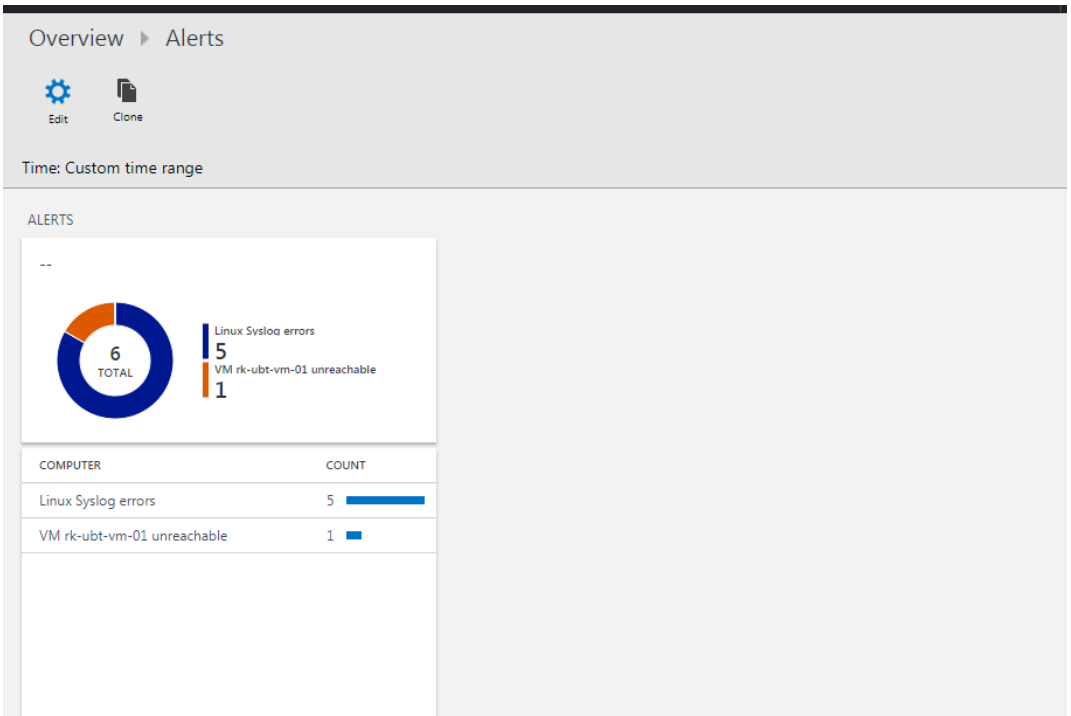


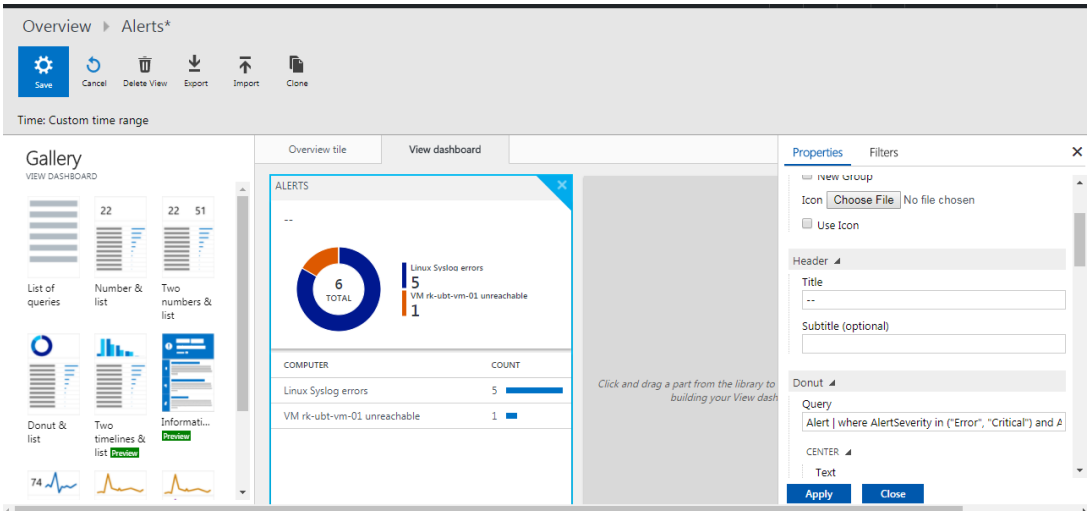
Some of the dashboards that you see in the screen above are standard dashboards that get imported with Solution Imports . The others we a custom dashboards. To create a new dashboard view you need to click on the Green plus button

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 [

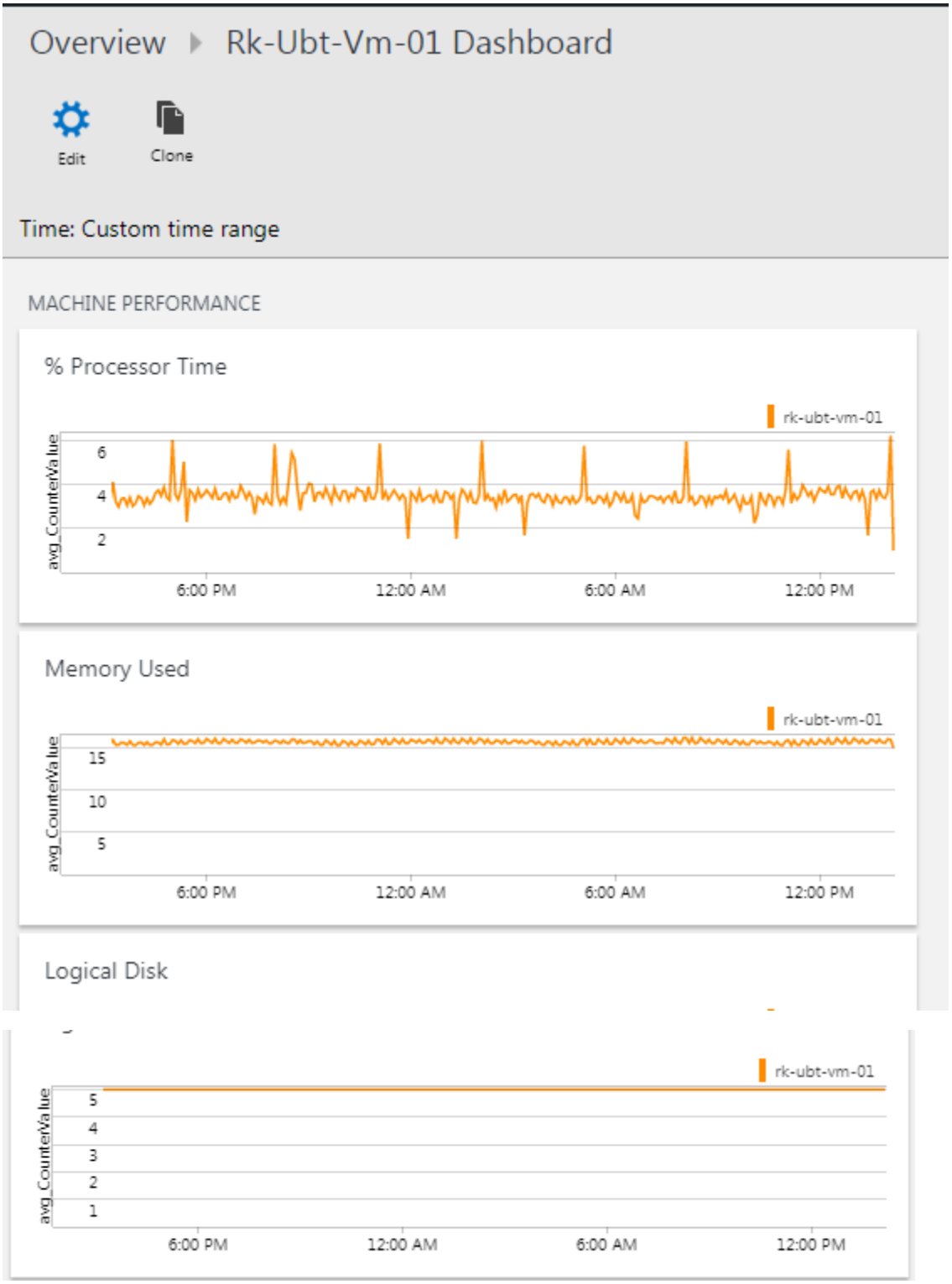
Alert Management Dashboard

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





Performance dashboard for VM

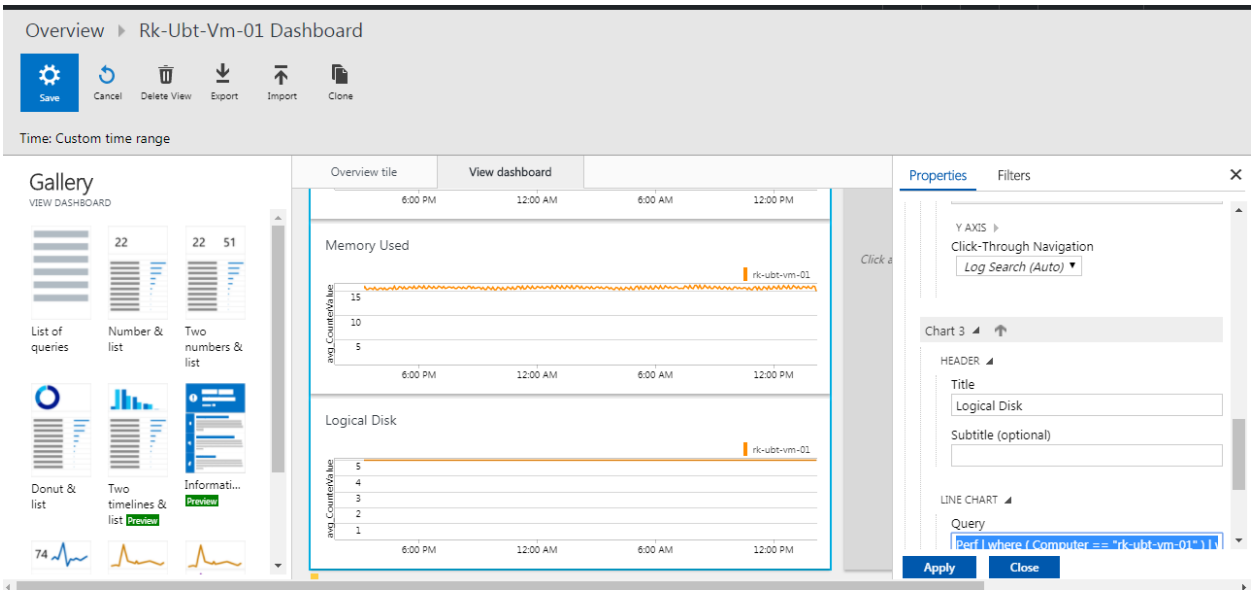


I used these queries

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

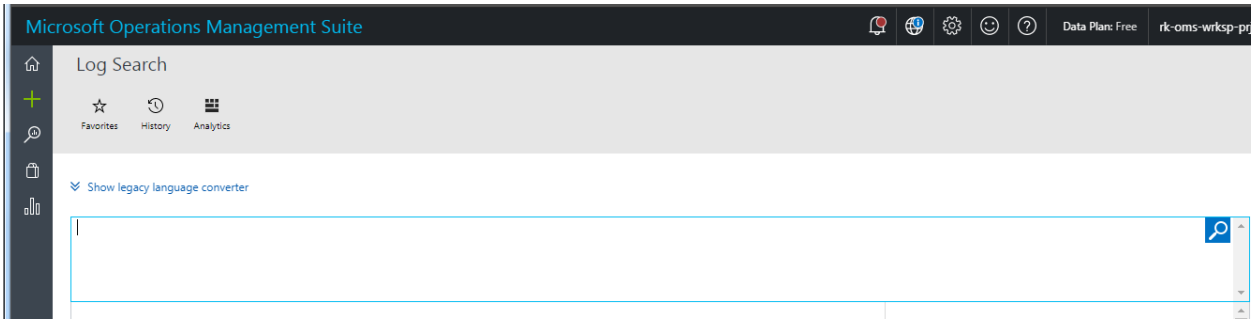
Perf | where (Computer == "rk-ubt-vm-01") | where (ObjectName == "Logical Disk") | where (CounterName == "% Used Space")| summarize avg(CounterValue) by Computer, bin(TimeGenerated, 5min)|render barchart

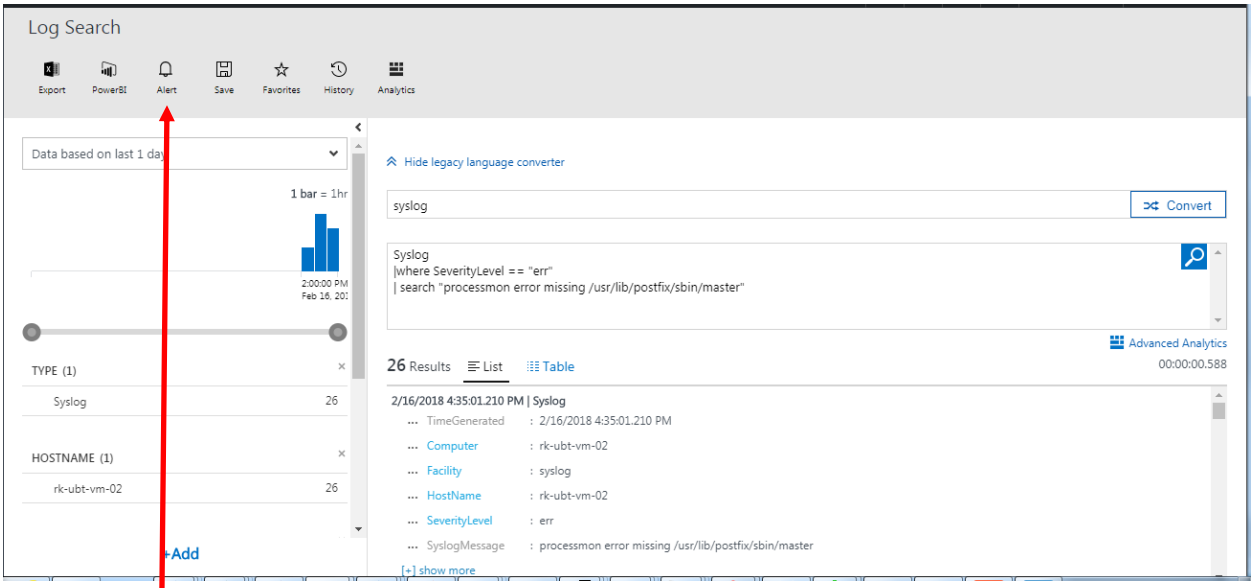


Alerts:

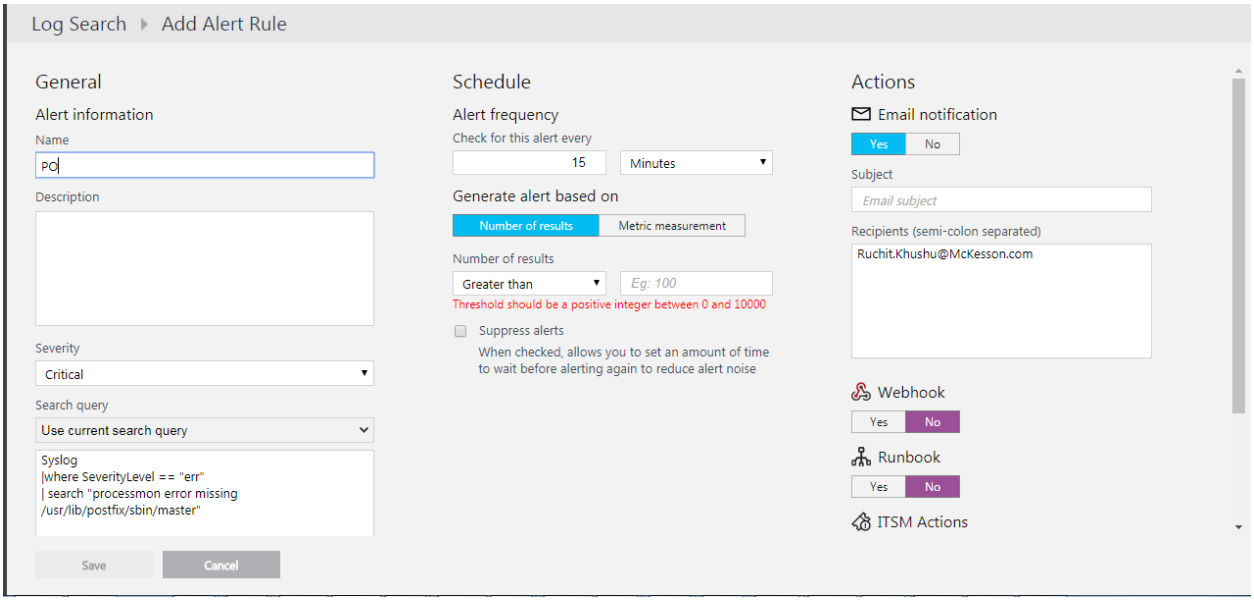
One of big advantages that Log Analytics provides is to set up Alerts . We can set up Alerts based on the output of the log queries.

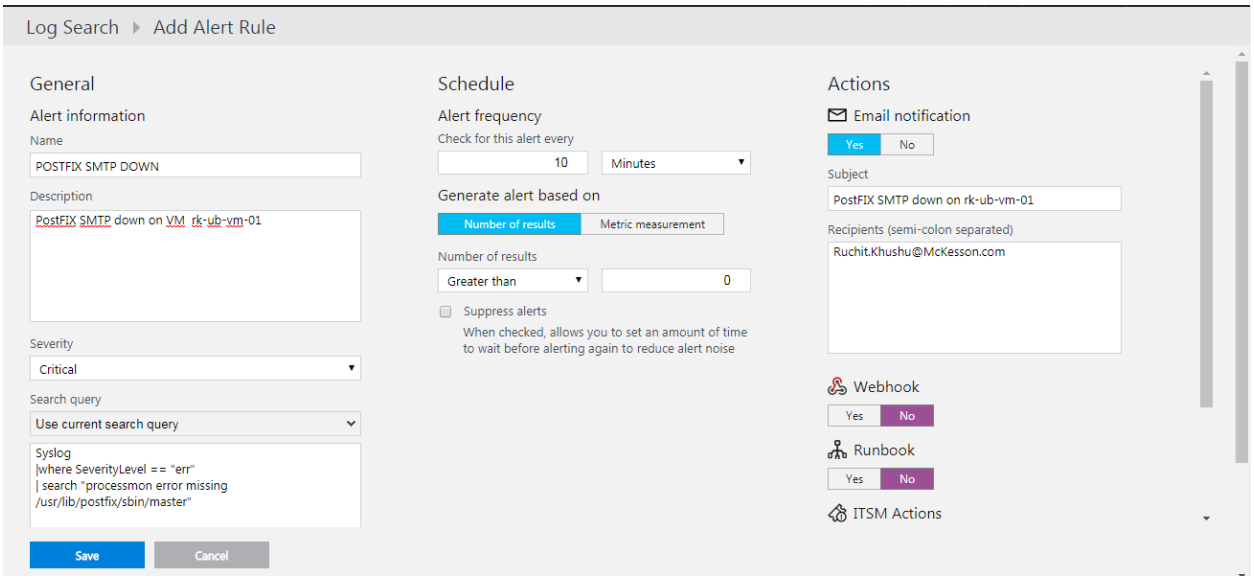
In order to create a new Alert please go the OMS Portal and in the log search section input the query for which Alerts needs to created





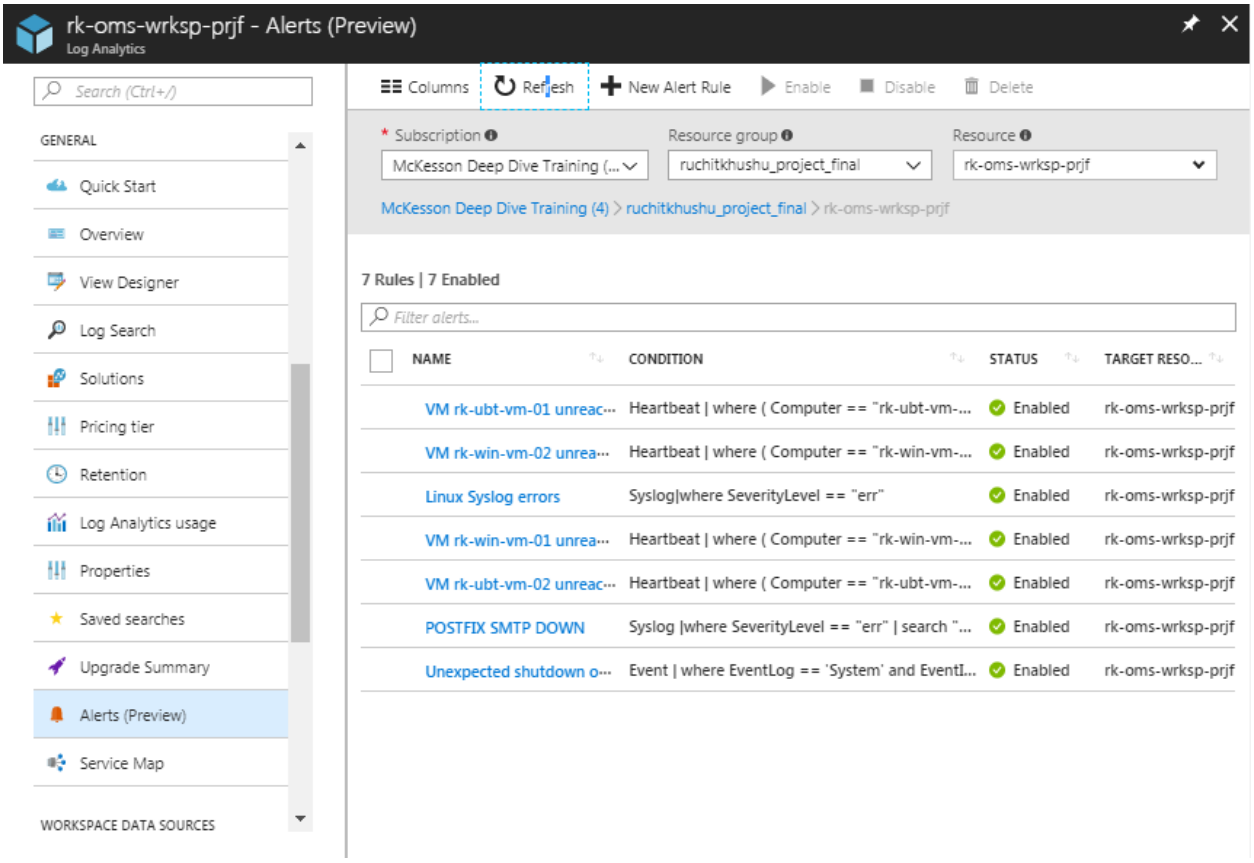
Click on the Alert button..On the next screen fill in the information…





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
McKesson Deep Dive Training (...
Resource group
ruchitkhushu_project_final
Resource
rk-oms-wrksp-prjf
McKesson Deep Dive Training (4) > ruchitkhushu_project_final > rk-oms-wrksp-prjf
7 Rules | 7 Enabled
Filter alerts...
NAME
CONDITION
STATUS
TARGET RESO...
VM rk-ubt-vm-01 unreac...
Heartbeat | where (Computer == "rk-ubt-vm-...
Enabled
rk-oms-wrksp-prjf
VM rk-win-vm-02 unrea...
Heartbeat | where (Computer == "rk-win-vm-...
Enabled
rk-oms-wrksp-prjf
Linux Syslog errors
Syslog|where SeverityLevel == "err"
Enabled
rk-oms-wrksp-prjf
VM rk-win-vm-01 unrea...
Heartbeat | where (Computer == "rk-win-vm-...
Enabled
rk-oms-wrksp-prjf
VM rk-ubt-vm-02 unreac...
Heartbeat | where (Computer == "rk-ubt-vm-...
Enabled
rk-oms-wrksp-prjf
POSTFIX SMTP DOWN
Syslog |where SeverityLevel == "err" | search "...
Enabled
rk-oms-wrksp-prjf
Unexpected shutdown o...
Event | where EventLog == 'System' and EventI...
Enabled
rk-oms-wrksp-prjf

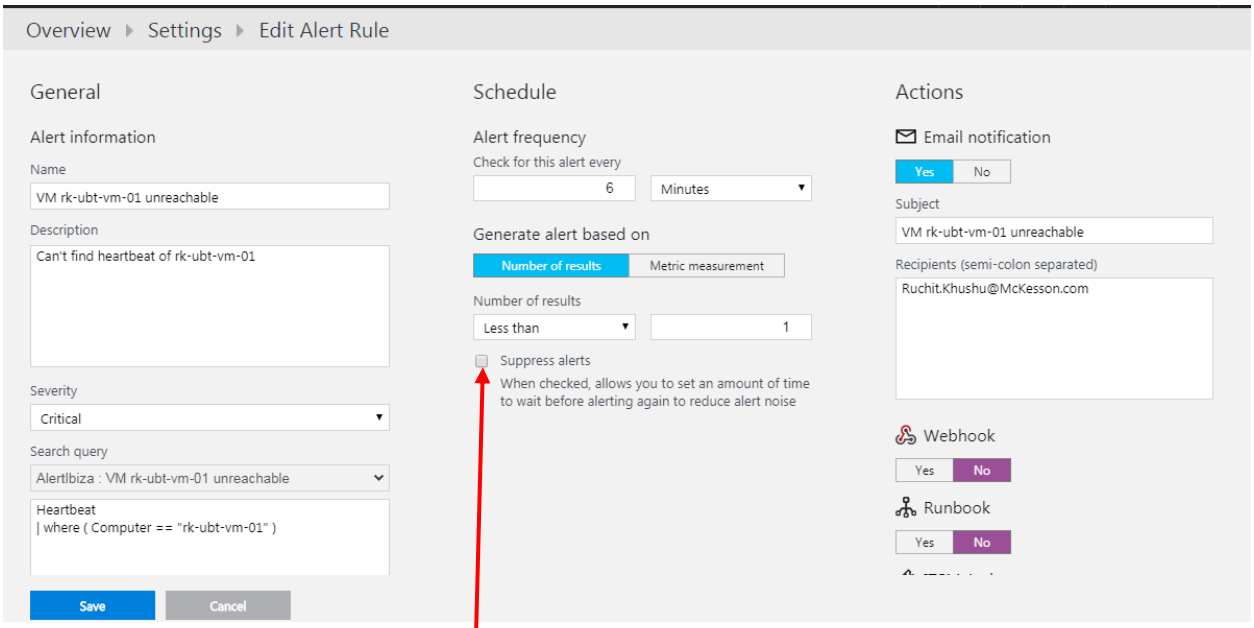
Custom Alerts

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:



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 | Move

N

Microsoft Operations Management Suite Team <noreply@oms.microsoft.com> | Khushu, 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.

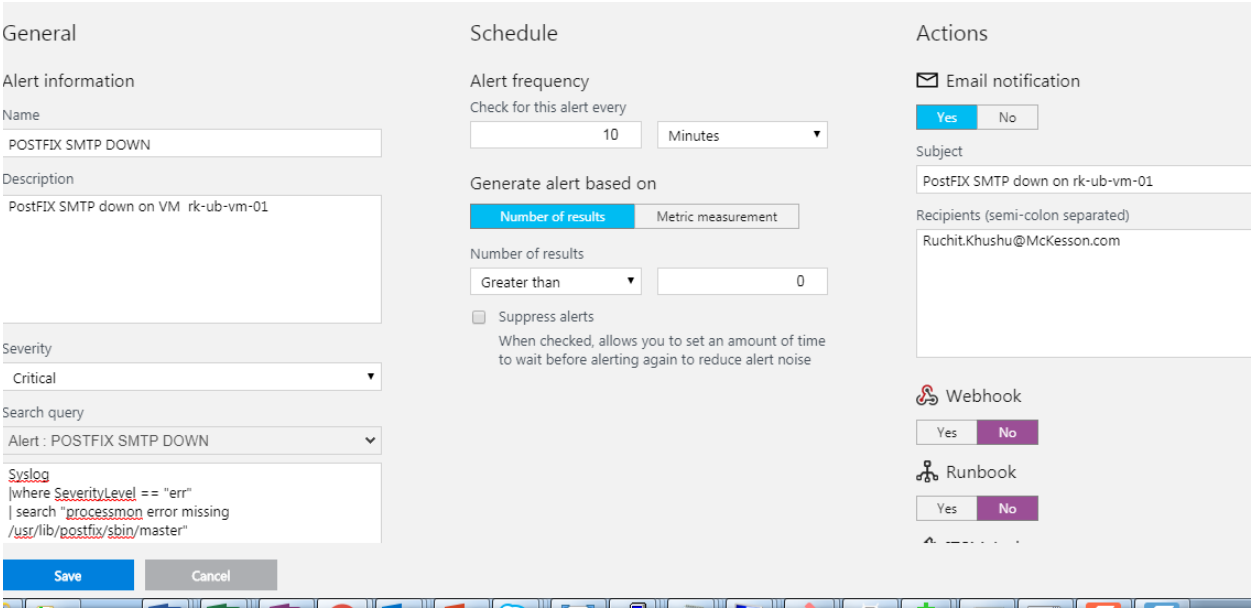
The query I used is:

Syslog

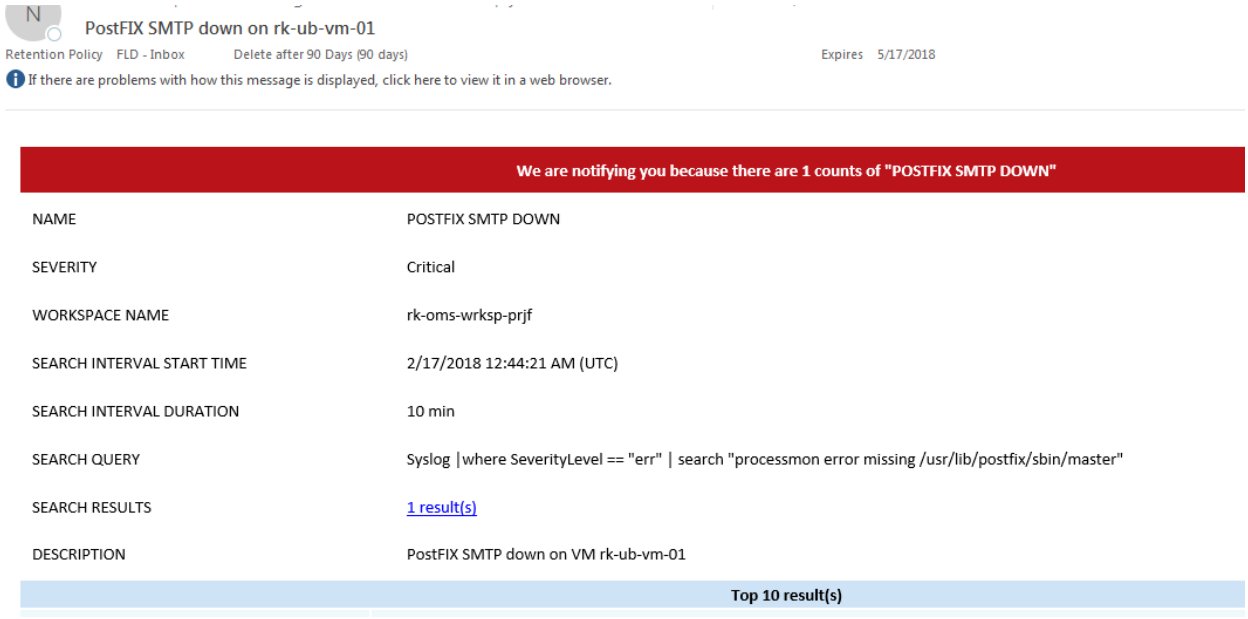
|where SeverityLevel == "err"

| 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 !!



And this is the email alert

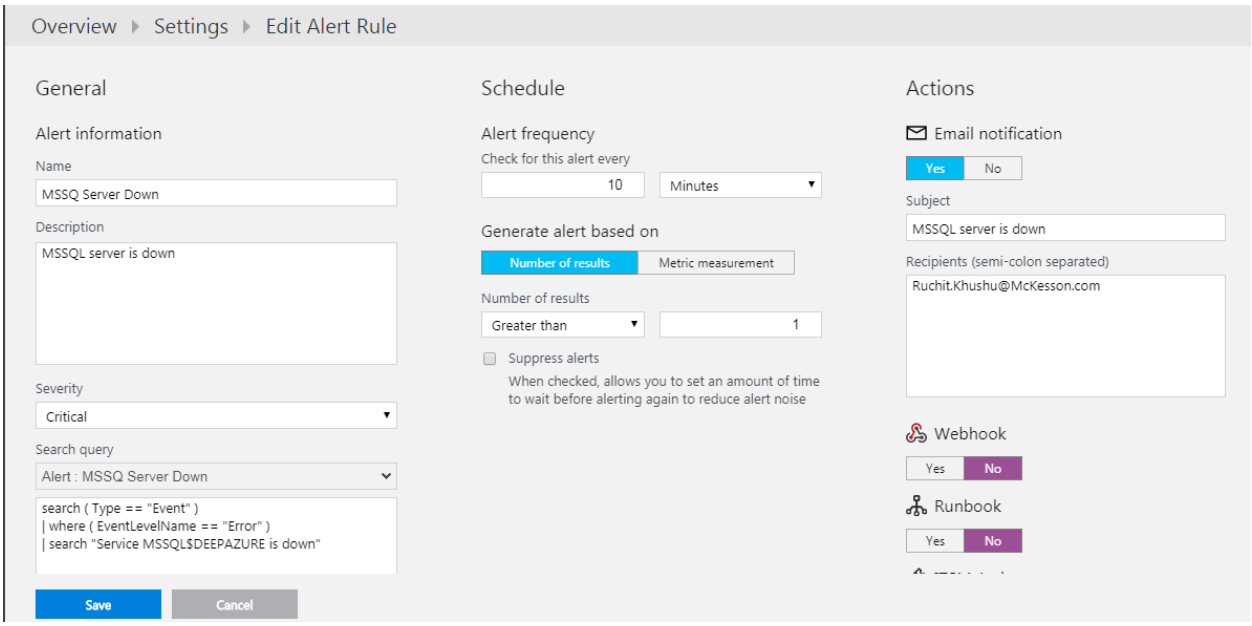


I have put the Linux shell script on Github as linuxprocmon.sh

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

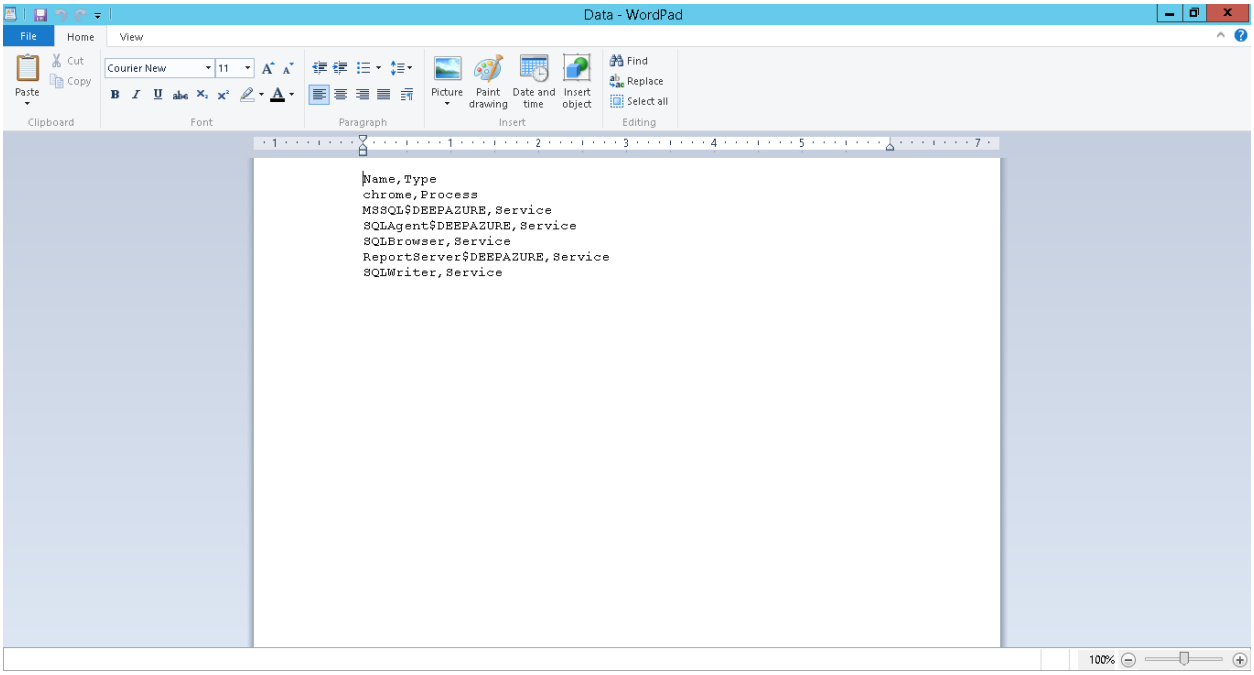


The following is the power shell script I built for this . It has to be run on the machine for which the monitoring has to be performed using Task scheduler . ***I have put the this service monitor power shell script on Github as winsvcmon.sh***

```
$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
}
```

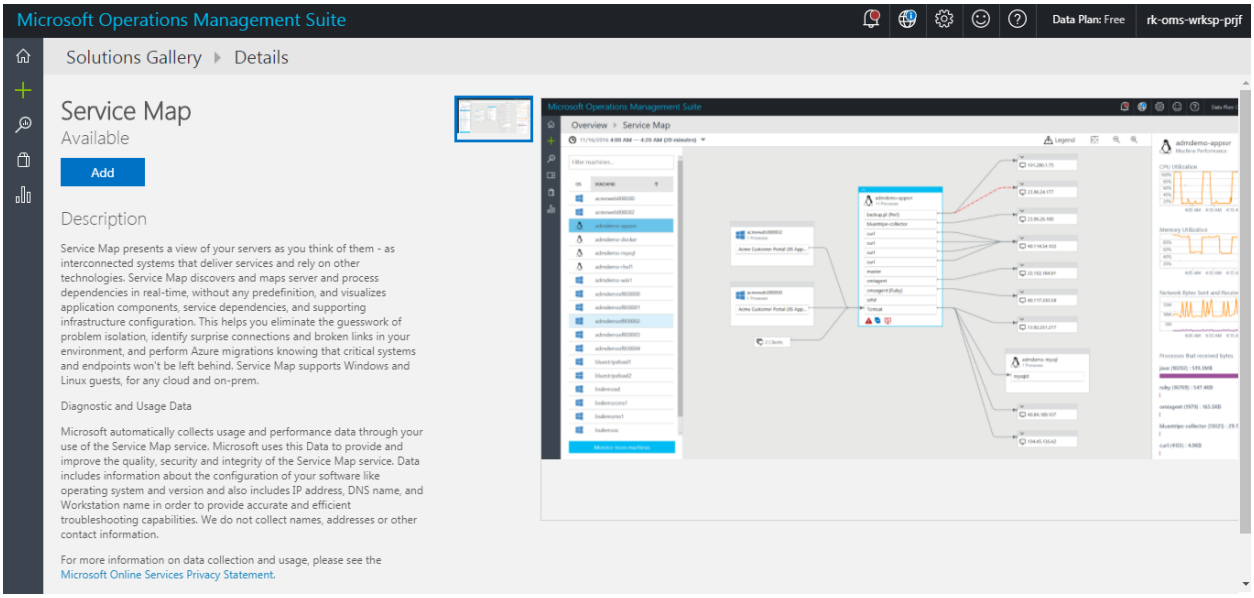
```
}

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:

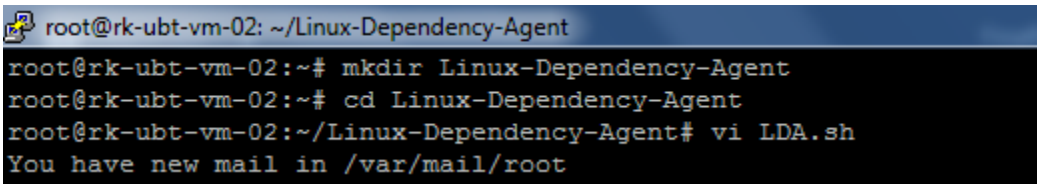


Service Map:

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

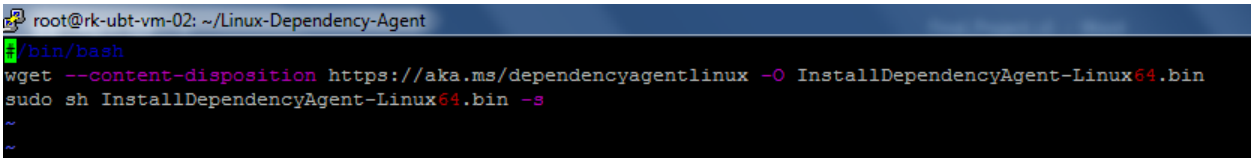


And then deloyed the Linux Dependency Agent on 1 on UBUNTU and 1 of my CENTOS VMs.



I created LDA.sh script with installation instructions

\



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#
```

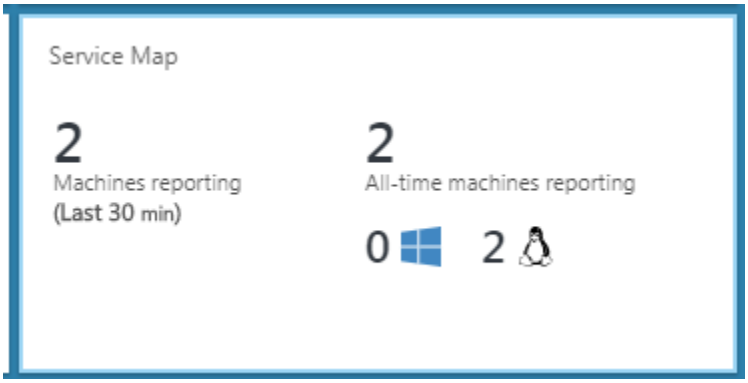
```
root@rk-cent-vm-01:~/Linux-Dependency-Agent
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 ~]# pwd
/root
[root@rk-cent-vm-01 ~]# mkdir Linux-Dependency-Agent
[root@rk-cent-vm-01 ~]# cd Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# vi LDAinstall.sh
[root@rk-cent-vm-01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

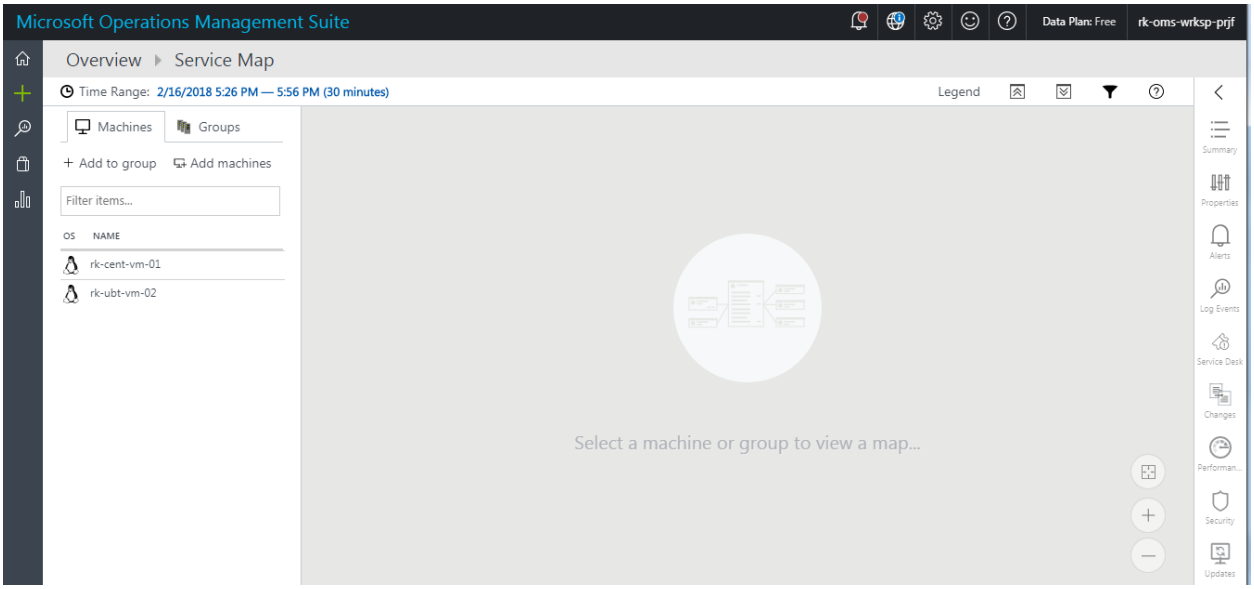
```
root@rk-cent-vm-01:~/Linux-Dependency-Agent
You have new mail in /var/spool/mail/root
[root@rk-cent-vm-01 ~]# pwd
/root
[root@rk-cent-vm-01 ~]# mkdir Linux-Dependency-Agent
[root@rk-cent-vm-01 ~]# cd Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# vi LDAinstall.sh
[root@rk-cent-vm-01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

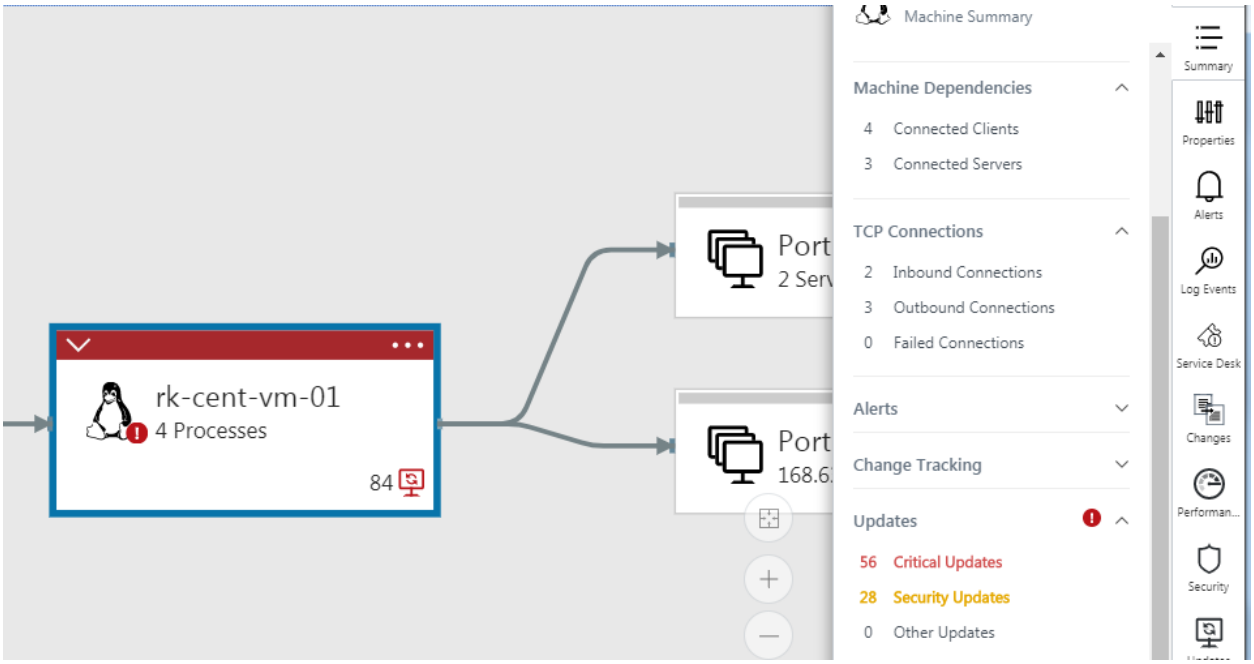
```
[root@rk-cent-vm-01 ~]# pwd
/root
[root@rk-cent-vm-01 ~]# mkdir Linux-Dependency-Agent
[root@rk-cent-vm-01 ~]# cd Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# vi LDAinstall.sh
[root@rk-cent-vm-01 Linux-Dependency-Agent]# chmod 755 LDAinstall.sh
You have new mail in /var/spool/mail/root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

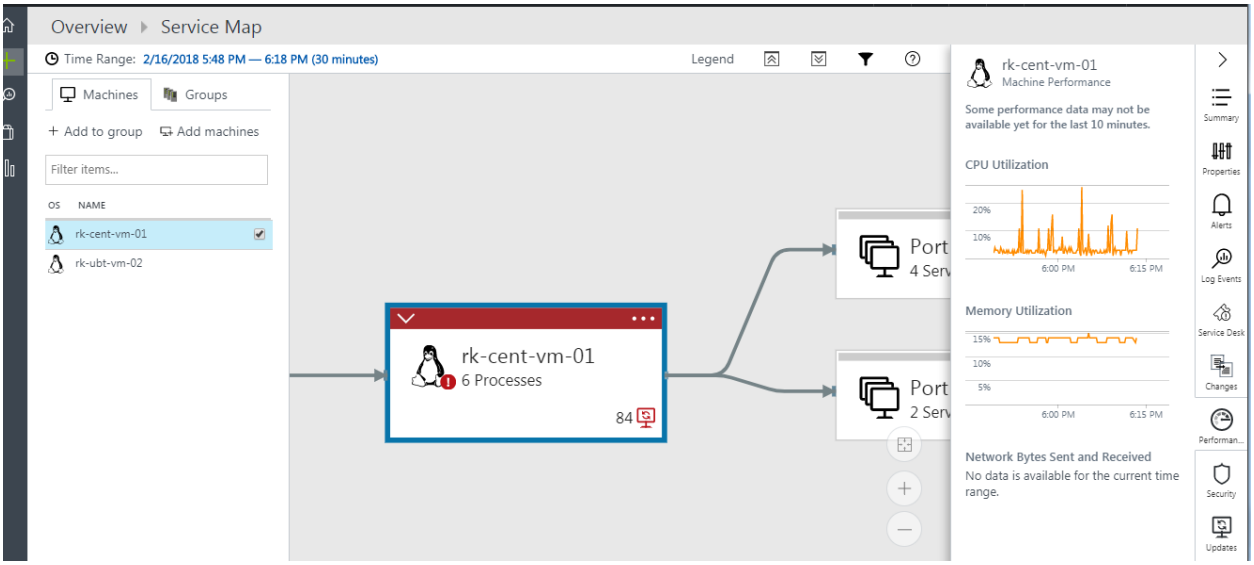
```
root@rk-cent-vm-01:~/Linux-Dependency-Agent
[root@rk-cent-vm-01 Linux-Dependency-Agent]# ps -ef|grep microsoft/dependency-agent
root      36106      1  0 08:33 pts/0    00:00:00 /bin/sh /opt/microsoft/dependency-agent/bin/microsoft-dependency-agent-manager
root      36148  36106  0 08:33 pts/0    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]#
```


Microsoft Operations Management Suite
Data based on custom time range
9
Total count of agents
0
Count of unresponsive agents in the last 24 hours
100
Active critical alerts in the last...
0
Active warning alerts in the la...
4pm 12pm 12am 4am 8am
100
TOTAL
Linux Syslog errors
44
VM rk-ubt-vm-01 unreachable
18
POSTFIX SMTP DOWN
16
Azure Automation
Enabled. Allows creation of Hybrid Runbook Workers for your Automation accounts.
ChangeTracking
298
ALL CHANGES
52
26
0
4:00 PM 8:00 PM 12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM
Device Health
Requires Configuration
This solution requires additional configuration. Please click here to complete all required configuration steps.
Network Performance Monitor
Data aggregation in progress
Network Performance Monitor is collecting data from your environment.
Note: Network Performance Monitor MUST be enabled on at least two machines for this process to succeed.
In some cases, first time data collection can take several hours to complete.
rk-ubt-vm-01 Dashboard
rk-ubt-vm-01
avg_CounterValue
6
4
2
12:00 AM
6:00 AM
12:00 PM
Service Map
2
Machines reporting
(Last 30 min)
2
All-time machines reporting
0
2
System Update Assessment


Service Map
2
Machines reporting
(Last 30 min)
2
All-time machines reporting
0
2


Microsoft Operations Management Suite
Data Plan: Free
rk-oms-wrksp-prjf
Overview
Service Map
Time Range: 2/16/2018 5:26 PM — 5:56 PM (30 minutes)
Legend
Machines
Groups
+ Add to group
Add machines
Filter items...
OS
NAME
rk-cent-vm-01
rk-ubt-vm-02
Select a machine or group to view a map...
Summary
Properties
Alerts
Log Events
Service Desk
Changes
Performan...
Security
Updates


rk-cent-vm-01
4 Processes
84
Machine Summary
Machine Dependencies
4 Connected Clients
3 Connected Servers
TCP Connections
2 Inbound Connections
3 Outbound Connections
0 Failed Connections
Alerts
Change Tracking
Updates
56 Critical Updates
28 Security Updates
0 Other Updates
Summary
Properties
Alerts
Log Events
Service Desk
Changes
Performan...
Security



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.