Contents

[AZURE MONITOR AND BACKUP 2](#_Toc134700809)

[AZURE MONITORS 2](#_Toc134700810)

[AZURE MONITORING – METRICES 2](#_Toc134700811)

[AZURE MONITORING – ACTIVITY LOGS 3](#_Toc134700812)

[AZURE MONITORING – ALERTS 3](#_Toc134700813)

[LOG ANALYTICS WORKSPACE 6](#_Toc134700814)

[CREATING A LOG ANALYTICS WORKSPACE 7](#_Toc134700815)

[CONNECTING A VM TO LOG ANALYTICS WORKSPACE 10](#_Toc134700816)

[LOG ANALYTICS QUERIES 11](#_Toc134700817)

# AZURE MONITOR AND BACKUP

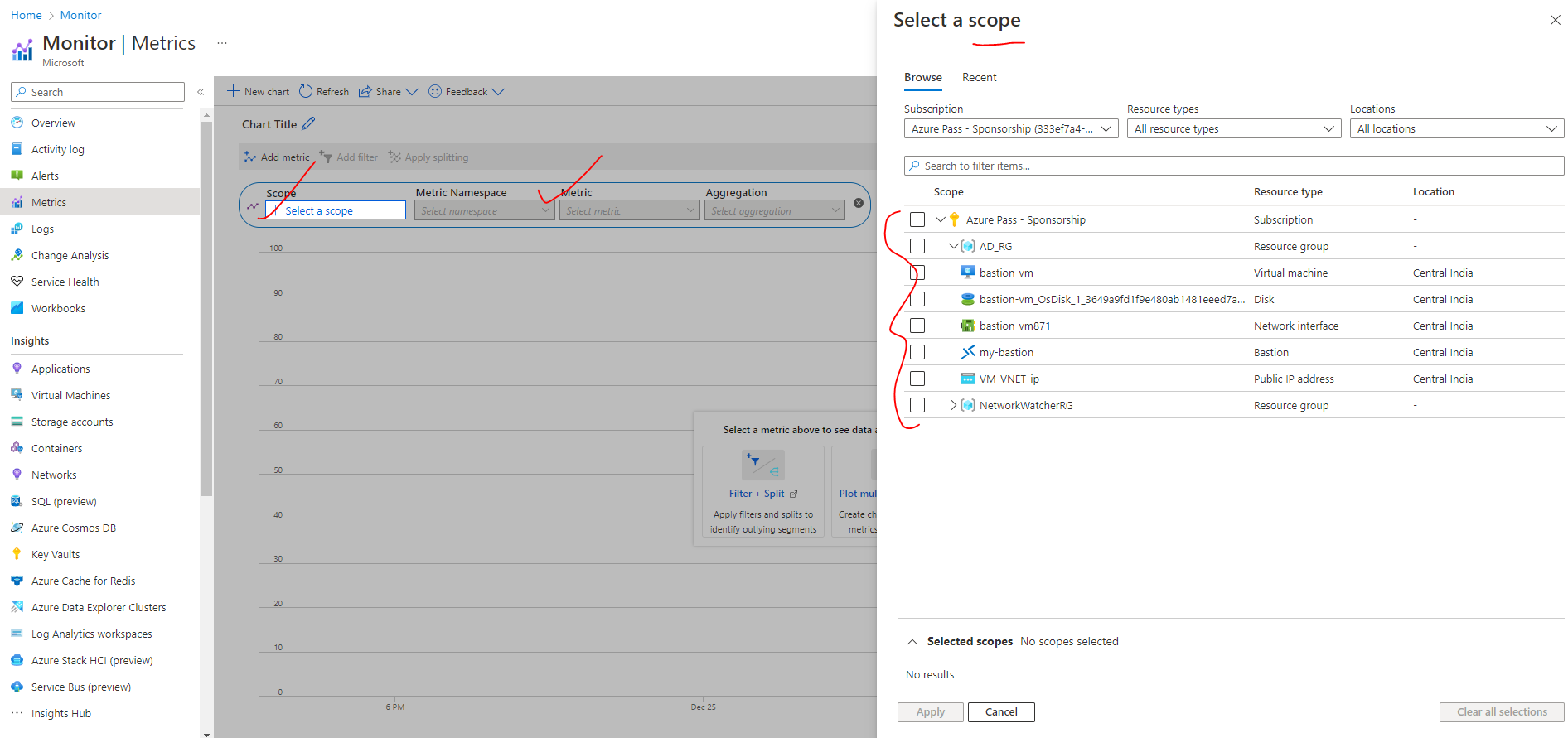
## AZURE MONITORS

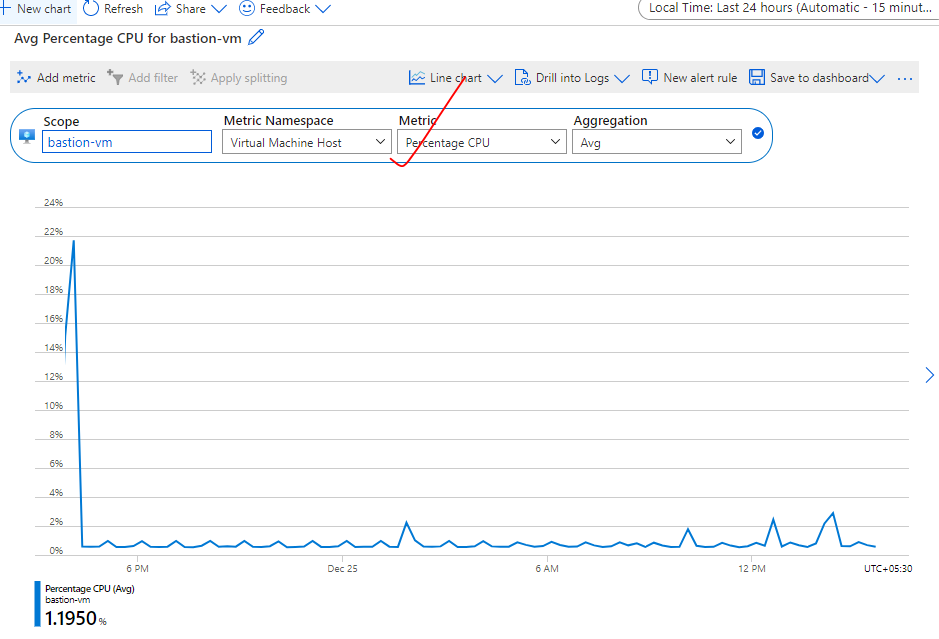
* Azure monitor has multiple aspects

|  |  |
| --- | --- |
| METRICES | * We can view the metrices of Azure resources. For example – For Azure VM , we can view CPU usage, Disk metrices , Network stats etc.. * We can create alerts of these metrices (For example – Sending an alert when CPU utilization go beyond certain threshold for a VM) |
| ACTIVITY LOGS | * Activity logs are for management activities on the Azure resource like Starting / Stopping the VMs, Creating VMs etc. * We can create alerts based on these activities |
| LOGS ANALYTICS WORKSPACE | * This the centralized solution for all logs in Azure * We can send application and resource logs to Log analytics workspace |
| APPLICATION INSIGHT | * Performance Management system of the live application. For example - Performance of the web app |

### AZURE MONITORING – METRICES

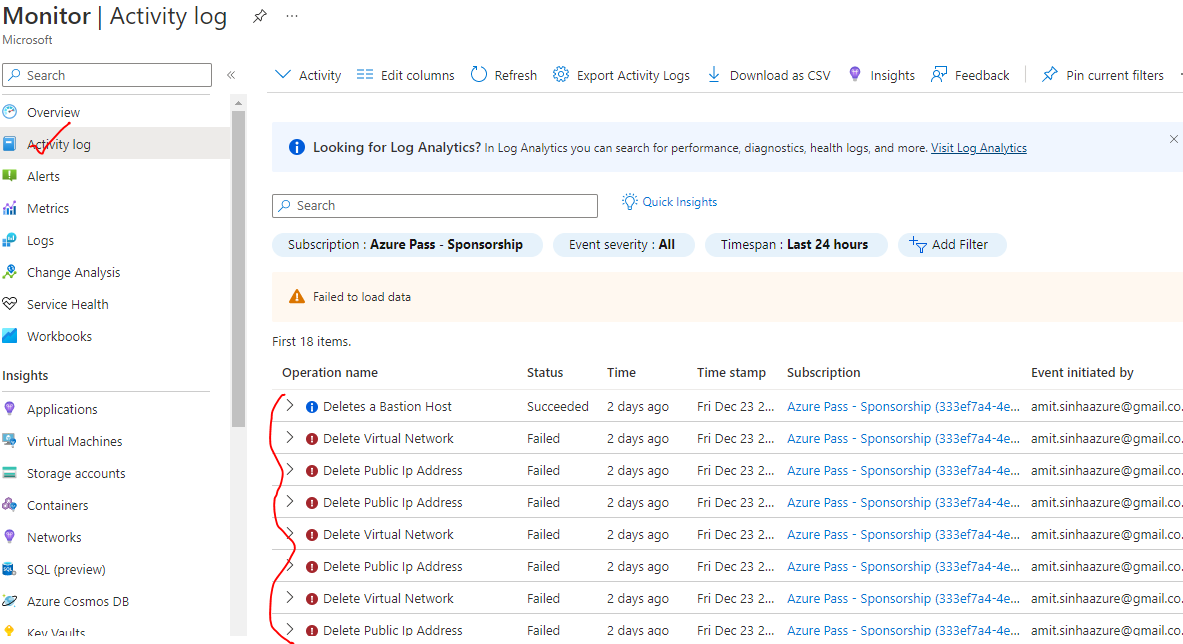
* To monitor any azure resources based on some metrices





### AZURE MONITORING – ACTIVITY LOGS

* Logs of control plane activity (administrator activity) for example Starting / Stopping /Deleting VM or deleting Storage Account

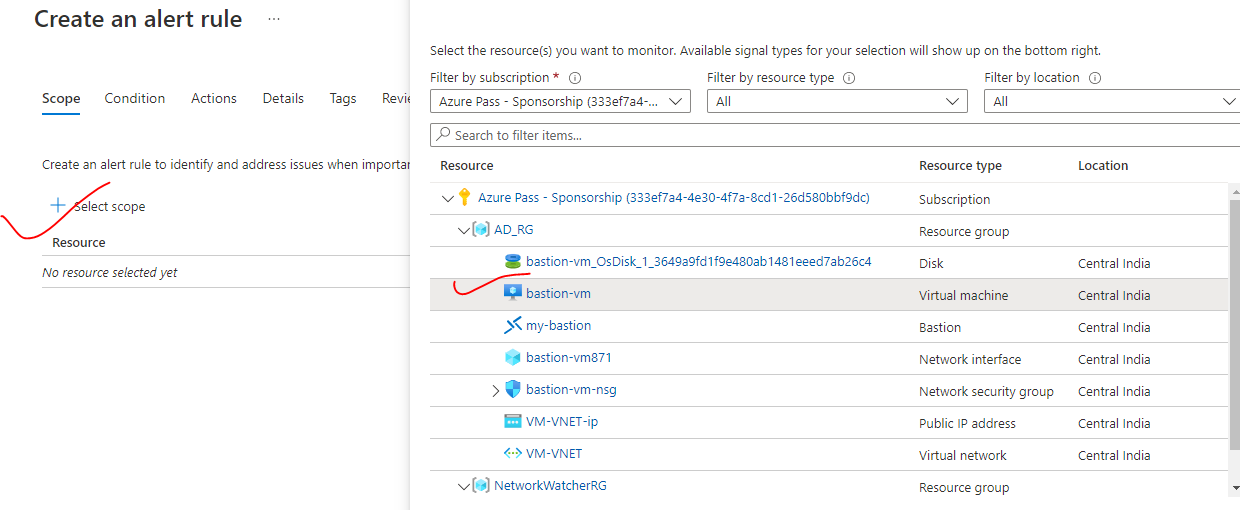


### AZURE MONITORING – ALERTS

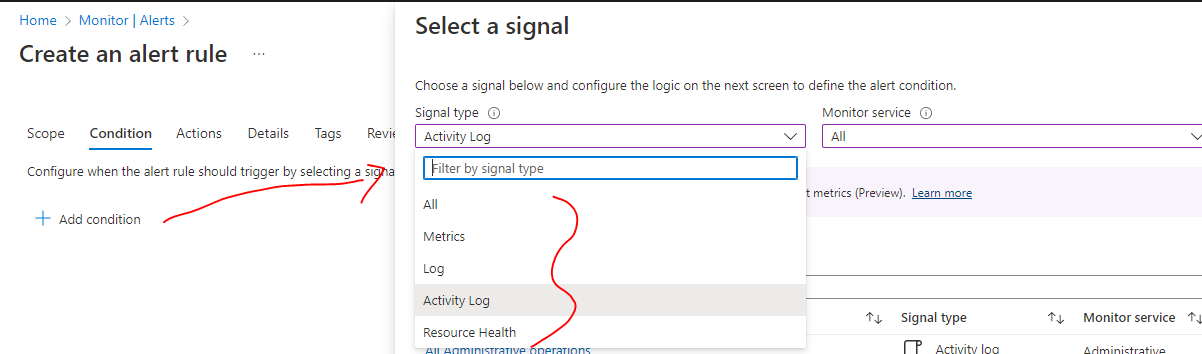
* We can create logs based on metrices or activity logs
* Monitors 🡪Create Rule



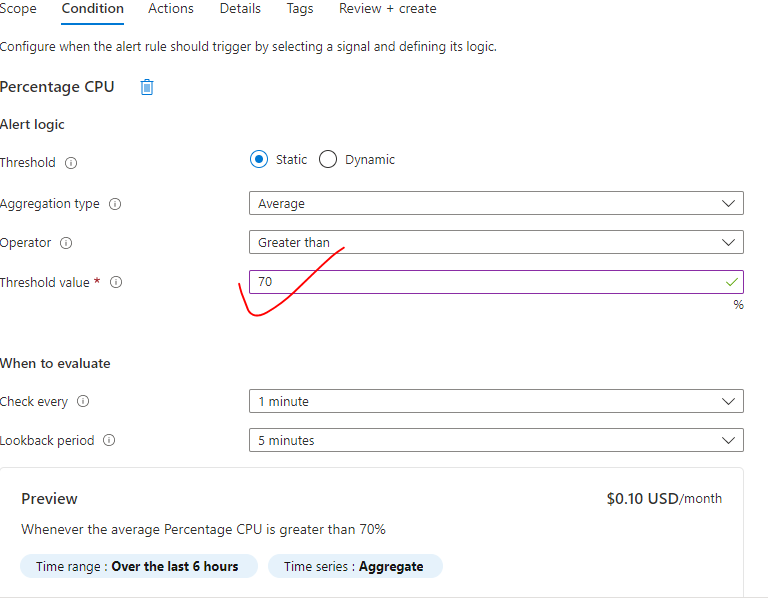
1. *STEP 1: SELECT THE SCOPE (AZURE RESOURCE TO BE MONITORED)*



1. *STEP 2: CREATE AN ALERT RULE (RULE ON WHICH WE WANT TO TRIGGER THE ALERT) – ALERT RULES CAN BE CREATED BASED ON METRICES/ ACTIVITY LOGS*

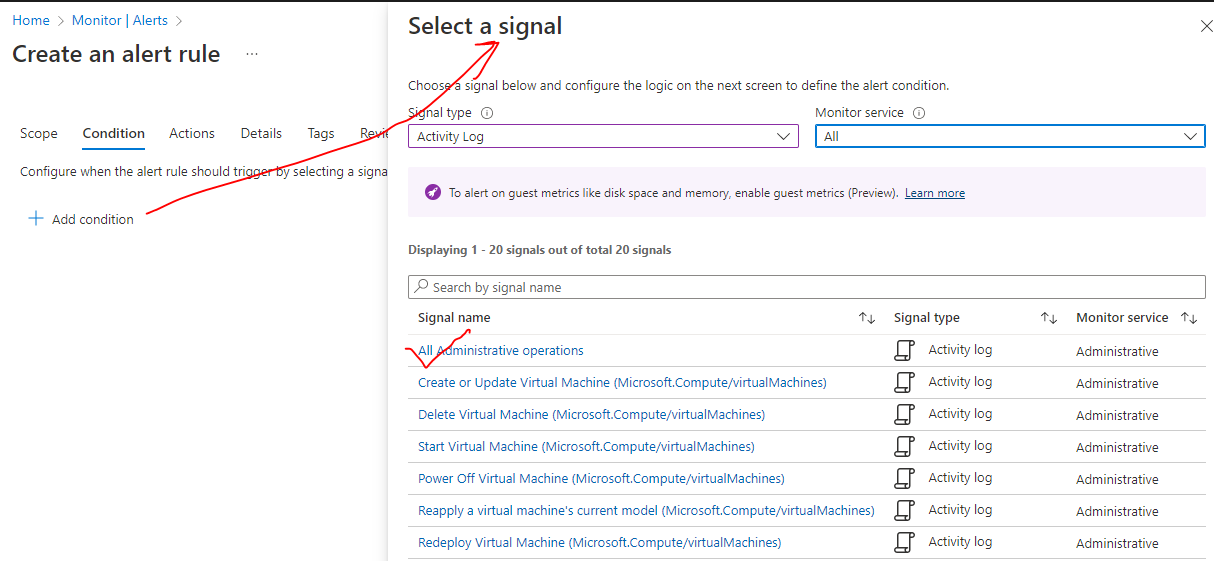


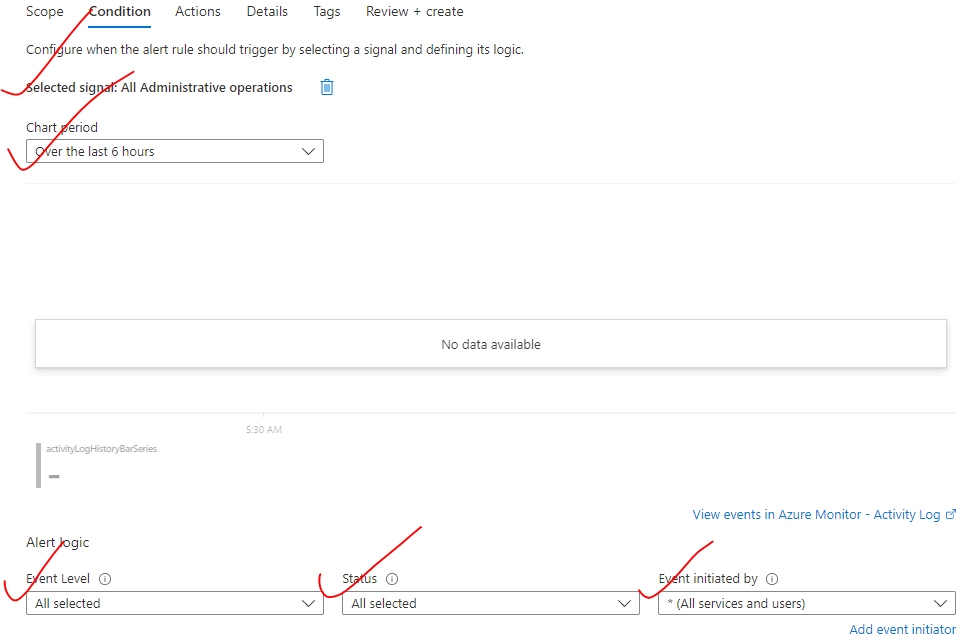
1. STEP 3: BASED ON METRICES (EXAMPLE – IF WANT TO TRIGGER THE ALERT WHEN CPU PERCENTAGE GO BEYOND 70%)



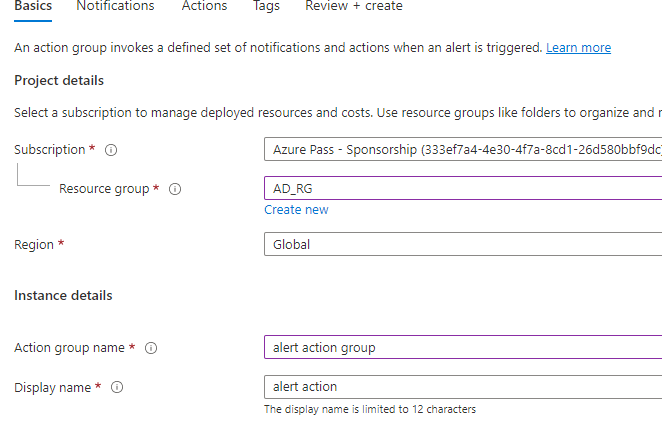
|  |  |
| --- | --- |
| Check every | Check the CPU utilization metrices every 1 min |
| Loopback period | While checking the metrices – consider the time span of last 5 mins |

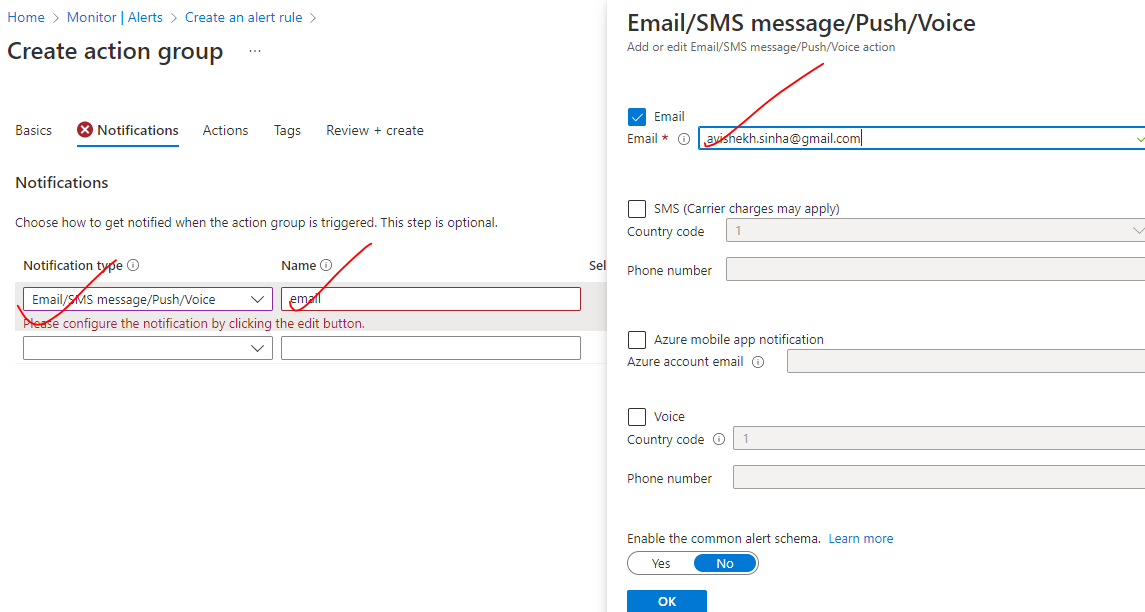
1. *STEP 4: BASED ON ADMIN OPERATIONS*



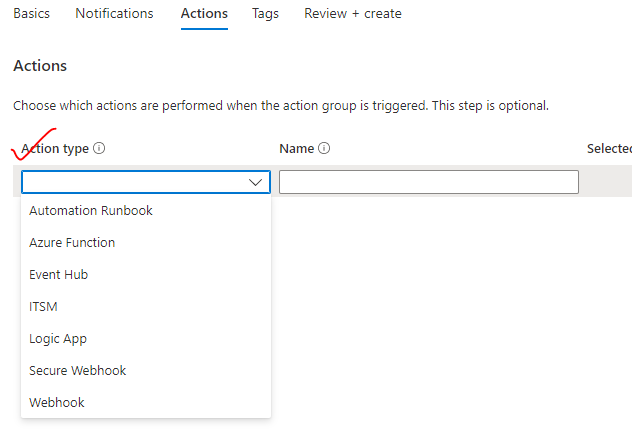


1. STEP 5: CREATE ACTION GROUP (ACTION TO BE PERFORMED

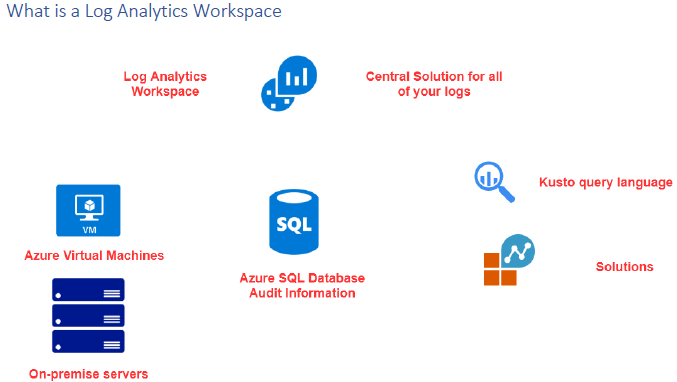




We can configure the notification to external system as well



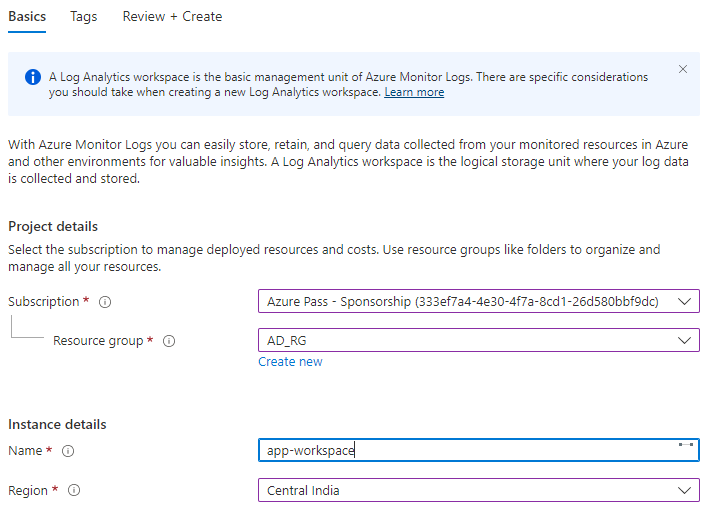
## LOG ANALYTICS WORKSPACE

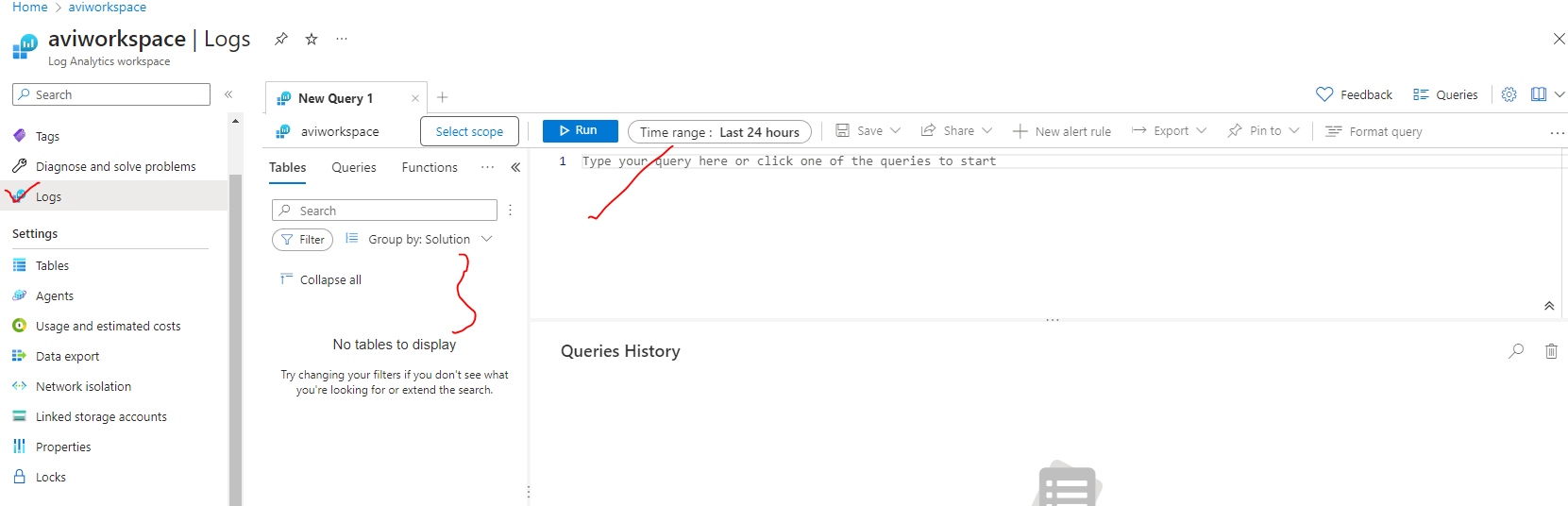


* Centralized solution of all Azure logs
* For example – let say we have resources like Azure VMs or a in premise servers – We can configure them to send the data to the log analytics workspace.
* Once we have the data available in the workspace, we can use a *Kusto query language* to perform queries to fetch the logged data

### CREATING A LOG ANALYTICS WORKSPACE

* Search and create “Log Analytics workspace”. Note As it a central logging system - the workspace can be created in any region (independent of the location the resources of which logging will captured) 🡪 Review +Create
* To avoid the cross-region data transfer charges – it always better to create the workspace in the same region.





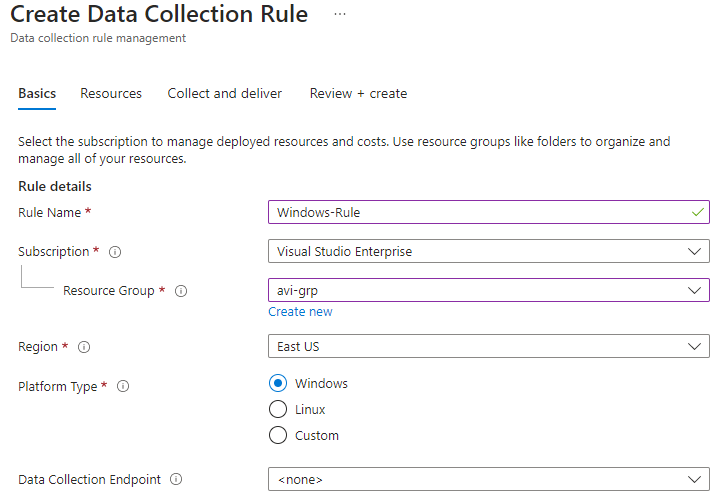
In the logs section

* On the left-hand side - We ideally see is some tables having log data.
* On the right-hand side, we can write queries against the data that are stored in the tables.

#### CREATING DATA COLLECTION

* Go to Azure Monitor Service 🡪 Data Collection Rules 🡪 Create

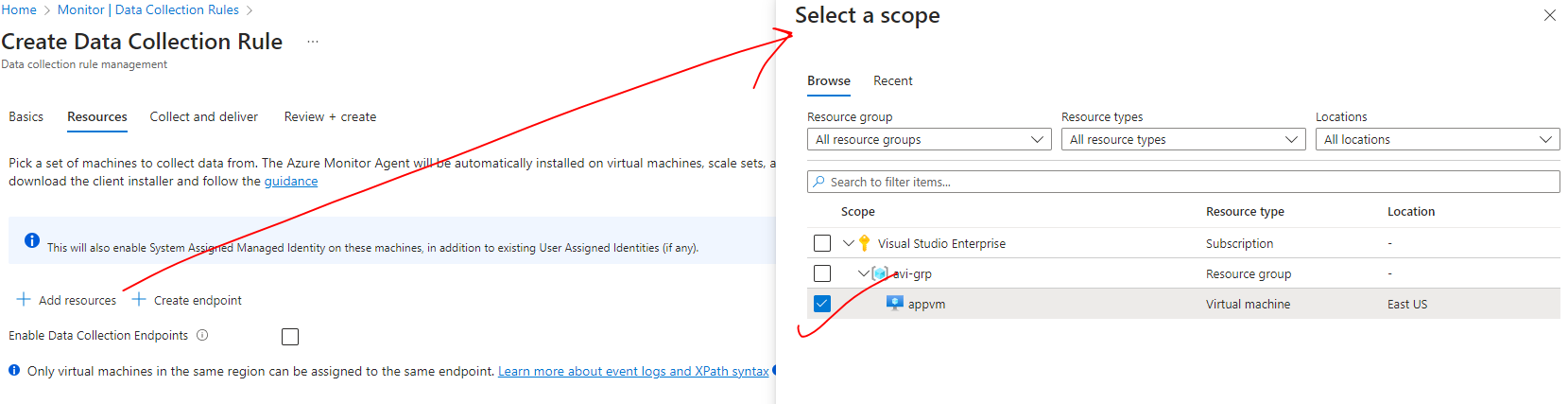
##### STEP 1: CONFIGURE DATA COLLECTION



* **PLATFORM TYPE**: The is the platform of the resource from where we want to collect the data/ logs from.

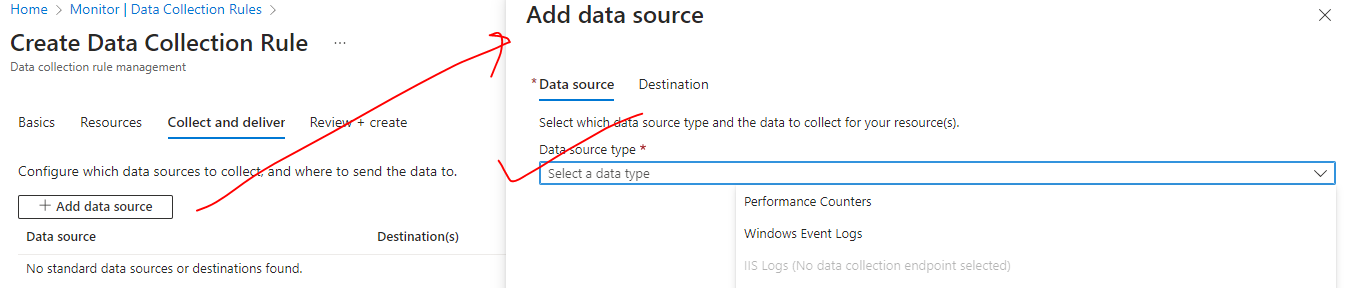
##### STEP 2: ADD THE RESOURCE

* Resource added for the data collection rule.



##### STEP 3: ADD THE DATA SOURCE

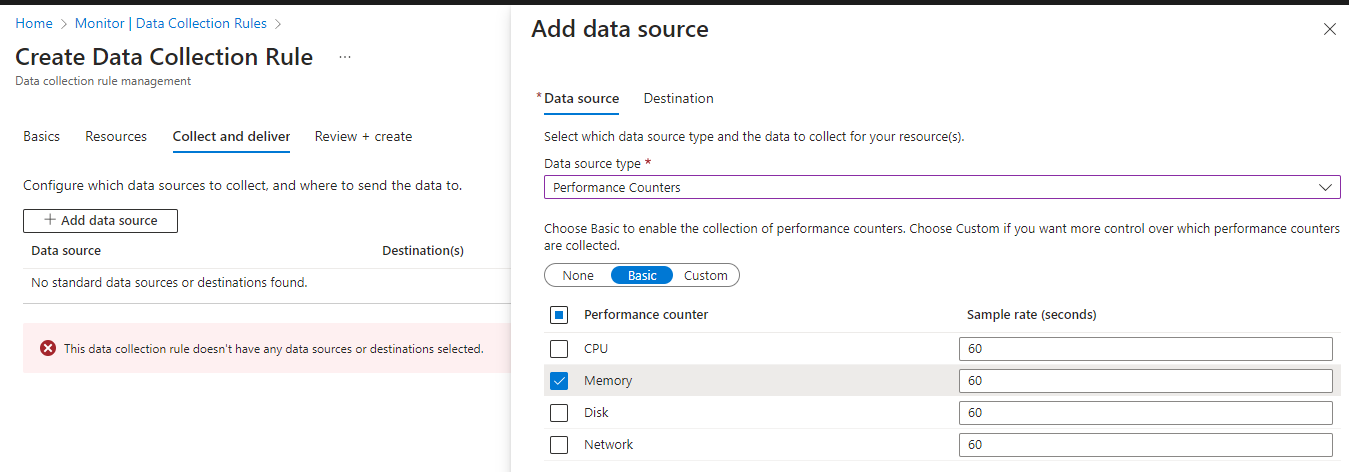
* In this step – we define what type of data we want to capture (Data Source Type)



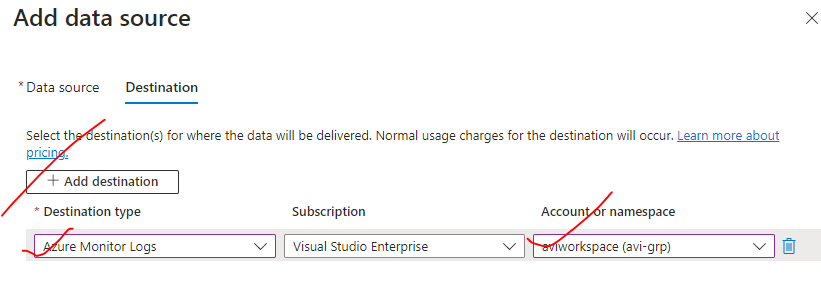
For example, for Windows VM - we have the option of choosing

|  |  |
| --- | --- |
| PERFORMANCE COUNTERS | * Performance counters is the performance metrics of the underlying Windows server. |
| WINDOWS EVENT LOGS | * Window OS Logs |

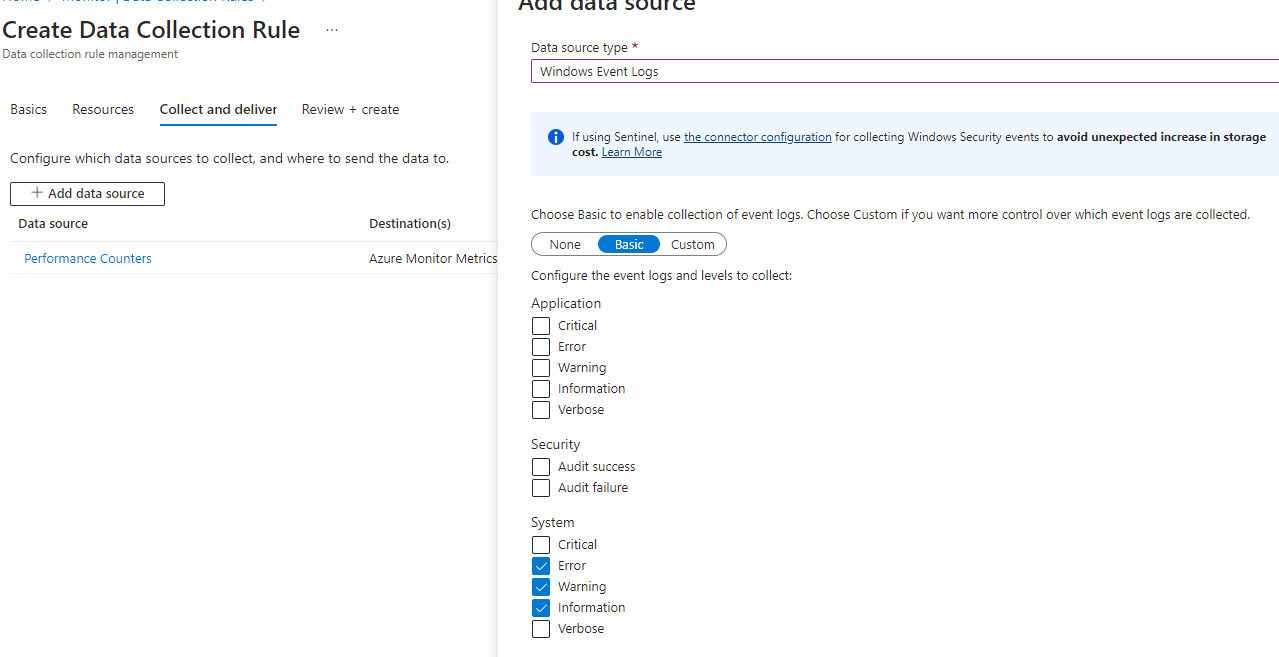
* Let’s select 🡪 Performance Counter. For now, let’s collect the data of Memory In Log Analytics
* Check “Memory” 🡪 Add data source



* Select the destination where want to send the logs to i.e Log Analytics work space 🡪 Save



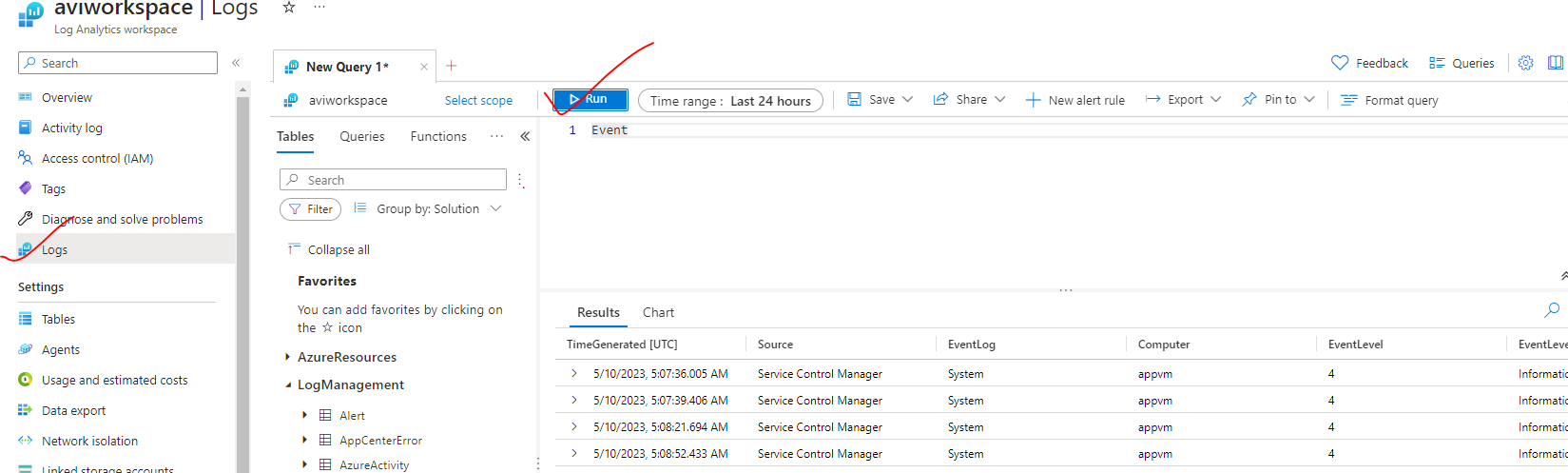
* If we want to collect Window logs data , then “Add Data Source” 🡪 Select the “Data Source type” as “Windows Event Logs” 🡪 select the desired options 🡪 Add Data Source



|  |  |
| --- | --- |
|  | * These are the 2 data source type we want to collect from Windows Based VM * In above use case – We configure the Monitor to collect the data for VM and send that data on to the log analytics workspace |

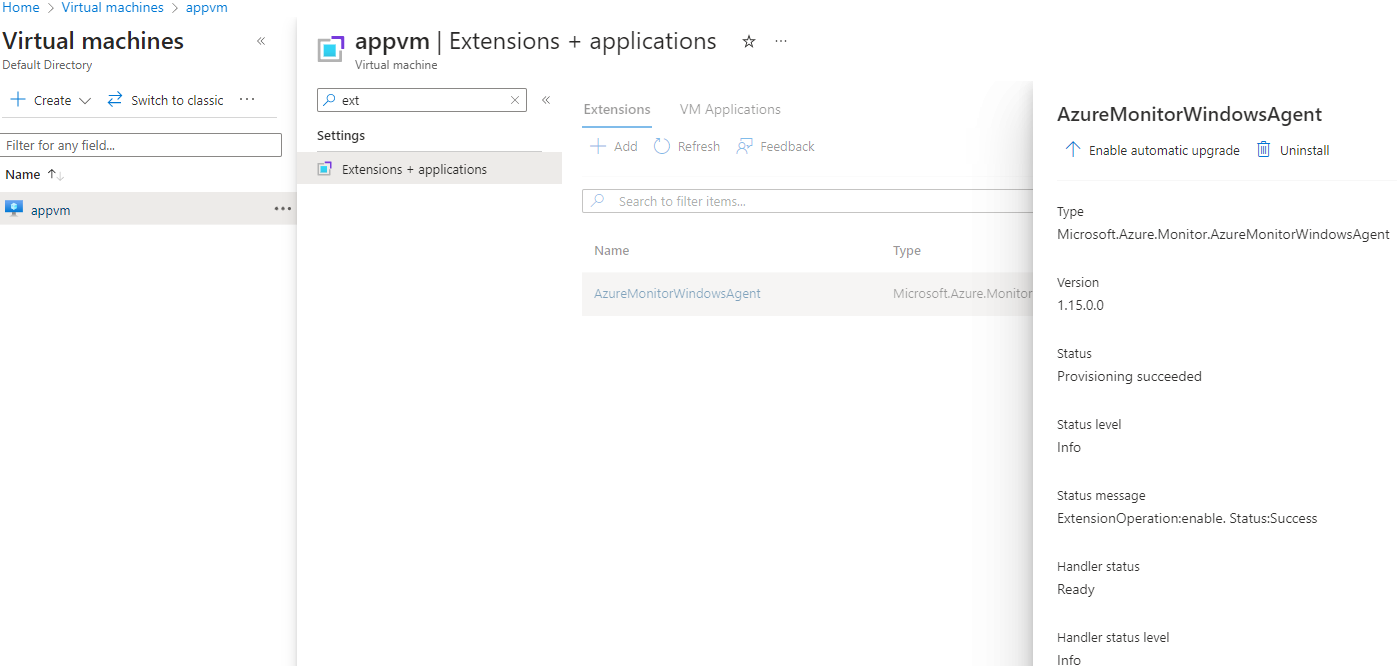
##### STEP 4: RUN QUERY TO FETCH THE LOGS

Go to Log Analytics Workspace 🡪 Logs



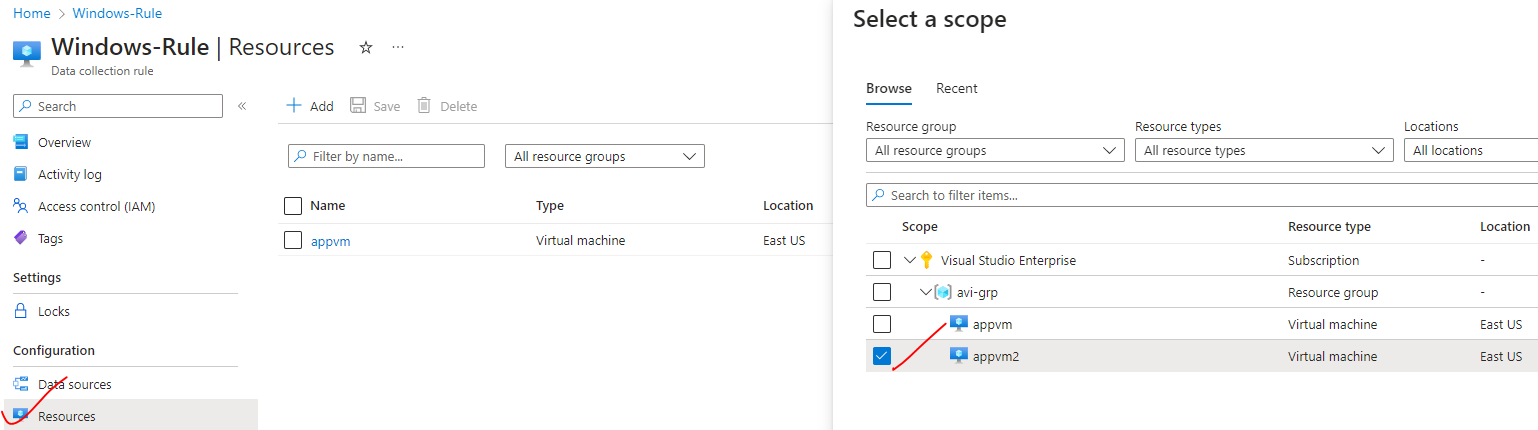
### CONNECTING A VM TO LOG ANALYTICS WORKSPACE

|  |  |
| --- | --- |
|  | * When you enable that feature of the data collection rule of sending data on to the log antics workspace, there is a Windows agent that gets installed. * To view the installed extension 🡪 Go to VM 🡪 Extension+ application |



#### ATTACHING A NEWLY CREATED VM WITH LOG ANALYTICS WORKSPACE

* We can attach a newly created VM(**appvm2**) to the log analytics workspace🡪 Go to the “Data Collection rule”
* Go to the Resource 🡪 Select the new VM to be added🡪 Apply



### LOG ANALYTICS QUERIES