Contents

[AZURE MONITOR AND BACKUP 2](#_Toc122890071)

[AZURE MONITORS 2](#_Toc122890072)

[AZURE MONITORING - METRICES 2](#_Toc122890073)

[AZURE MONITORING – ACTIVITY LOGS 3](#_Toc122890074)

[AZURE MONITORING – ALERTS 3](#_Toc122890075)

[LOG ANALYTICS WORKSPACE 6](#_Toc122890076)

[CREATING A LOG ANALYTICS WORKSPACE 7](#_Toc122890077)

[CONNECTING A VM TO LOG ANALYTICS WORKSPACE 7](#_Toc122890078)

# AZURE MONITOR AND BACKUP

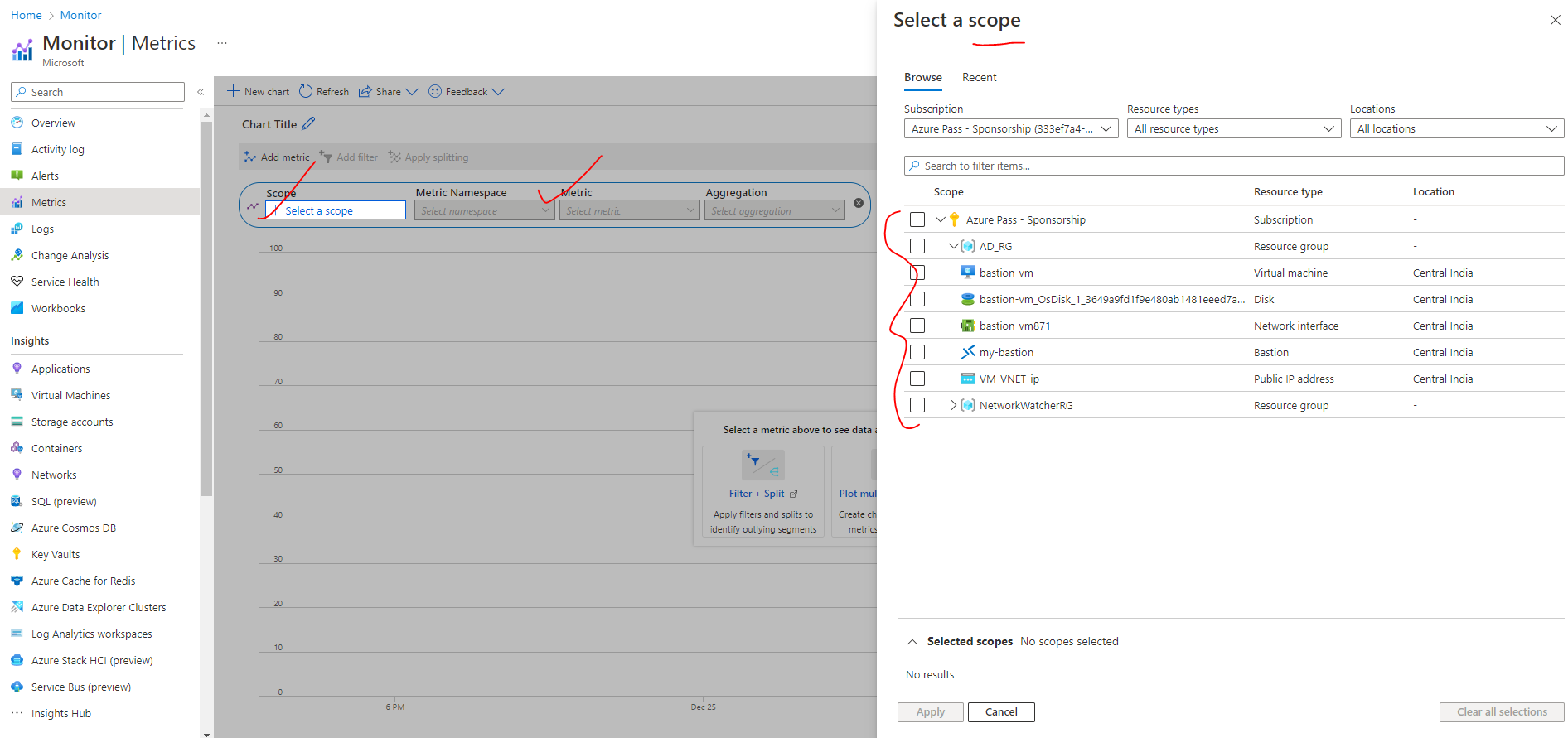
## AZURE MONITORS

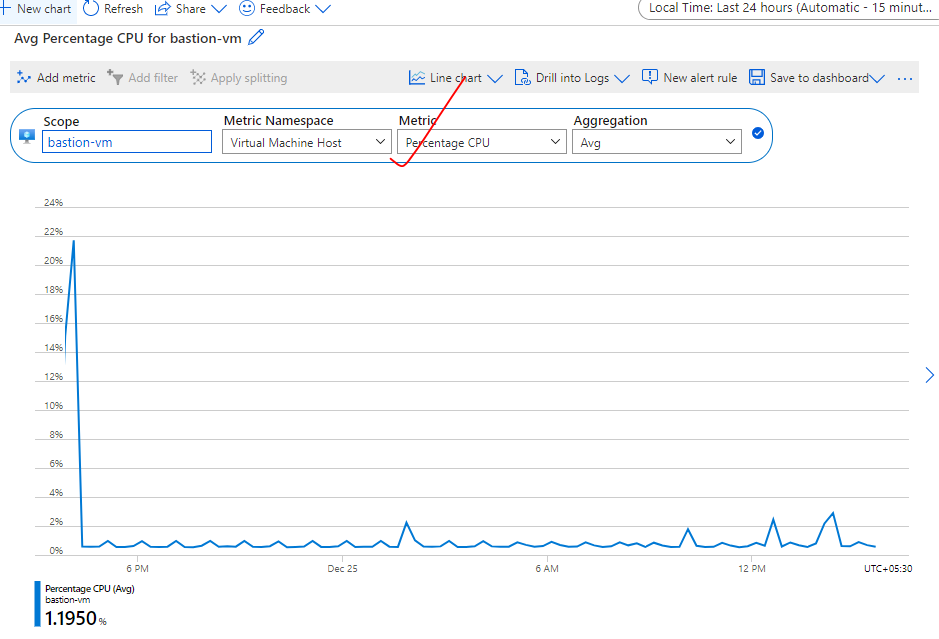
* Azure monitor has multiple aspects

|  |  |
| --- | --- |
| 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

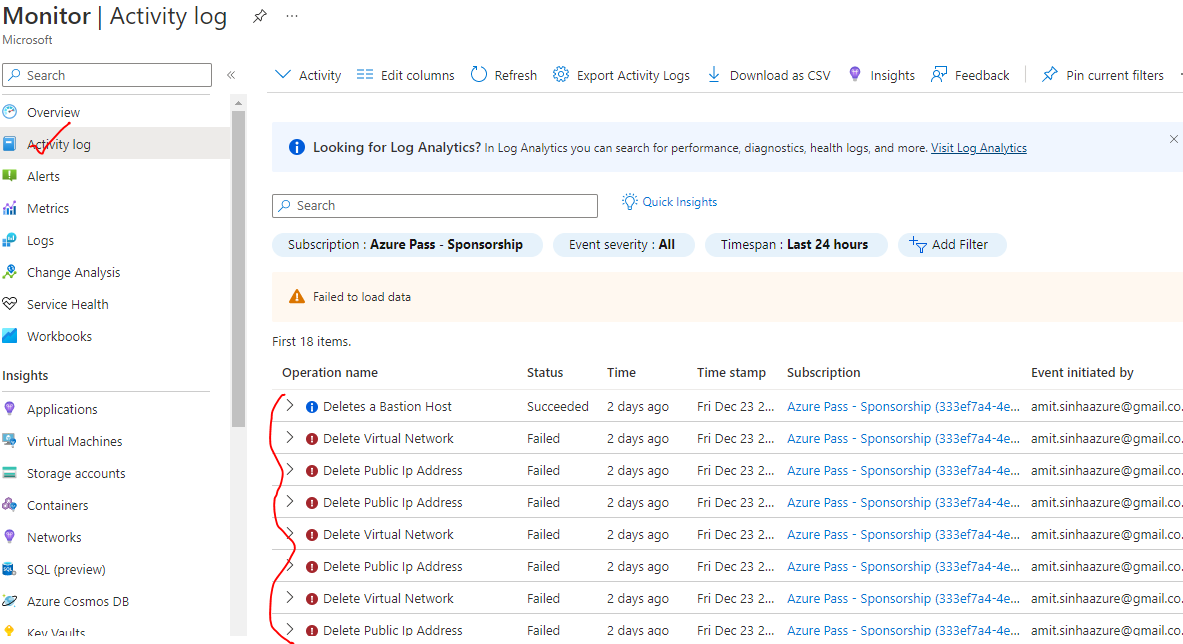
* To monitor any azure resources based on some metrices





### AZURE MONITORING – ACTIVITY LOGS

* Logs of control plane activity (administrator activity)

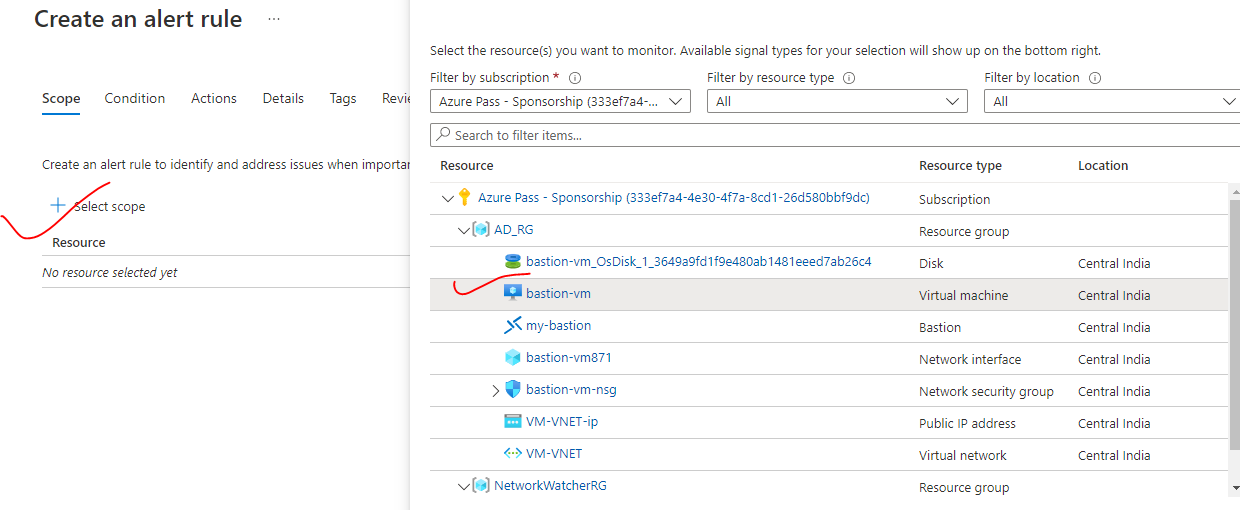


### AZURE MONITORING – ALERTS

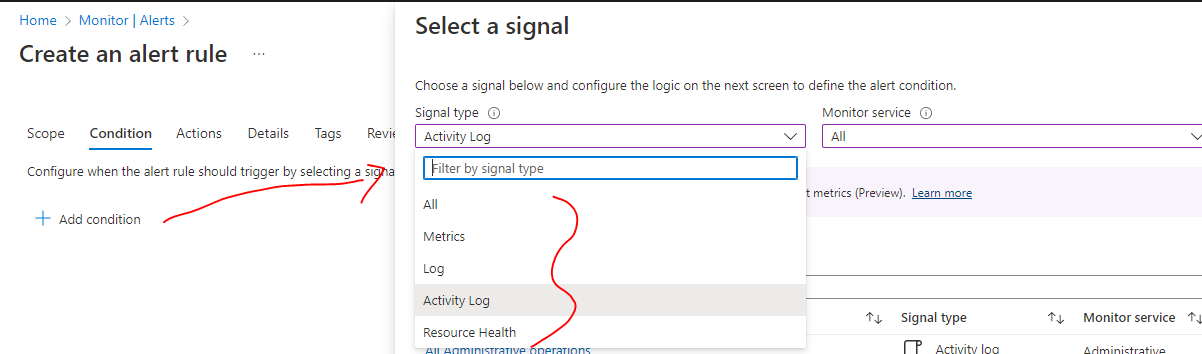
* We can create logs based on metrices or activity logs
* Monitors 🡪Create Rule



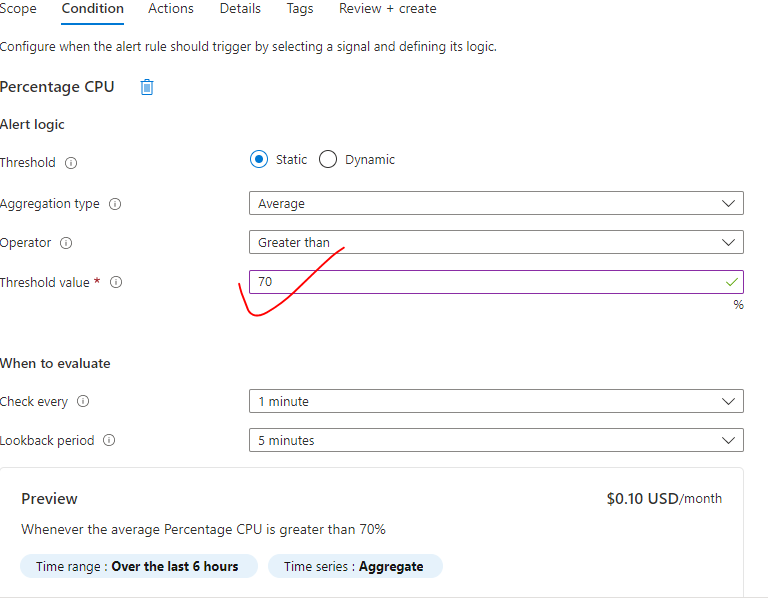
1. *STEP 1: SELECT THE SCOPE (AZURE RESOURCE TO BE MONITORED)*



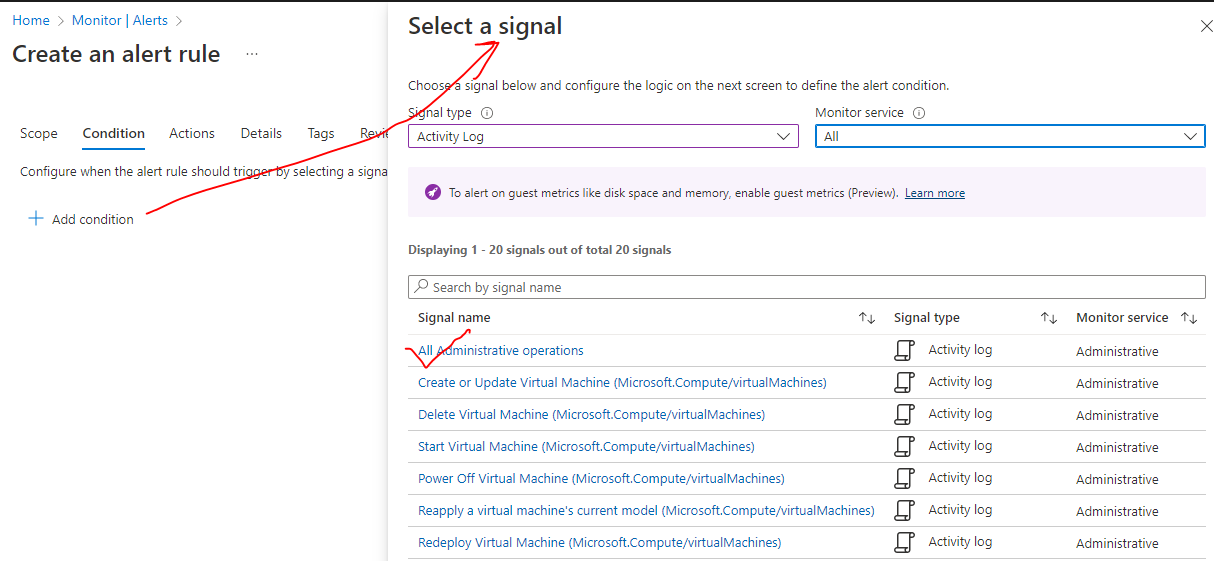
1. *STEP 2: CREATE AN ALERT RULE (RULE ON WHICH WE WANT TO TRIGGER THE ALERT) – ALERT RULES CAN BE CREATED BASED ON METRICES/ ACTIVITY LOGS*

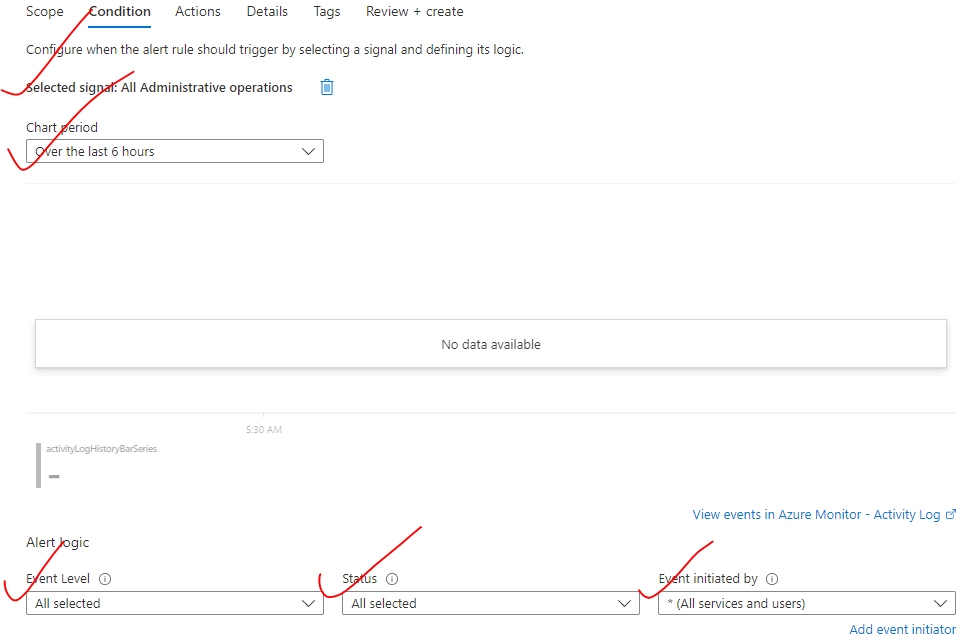


1. *STEP 3: BASED ON METRICES (EXAMPLE – IF WANT TO TRIGGER THE ALERT WHEN CPU PERCENTAGE GO BEYOND 70%)*

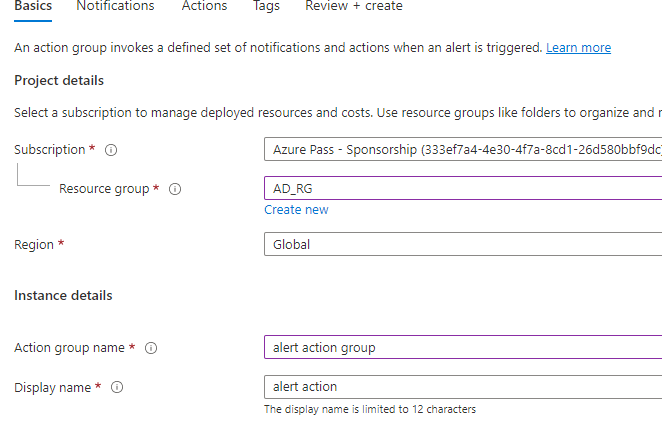


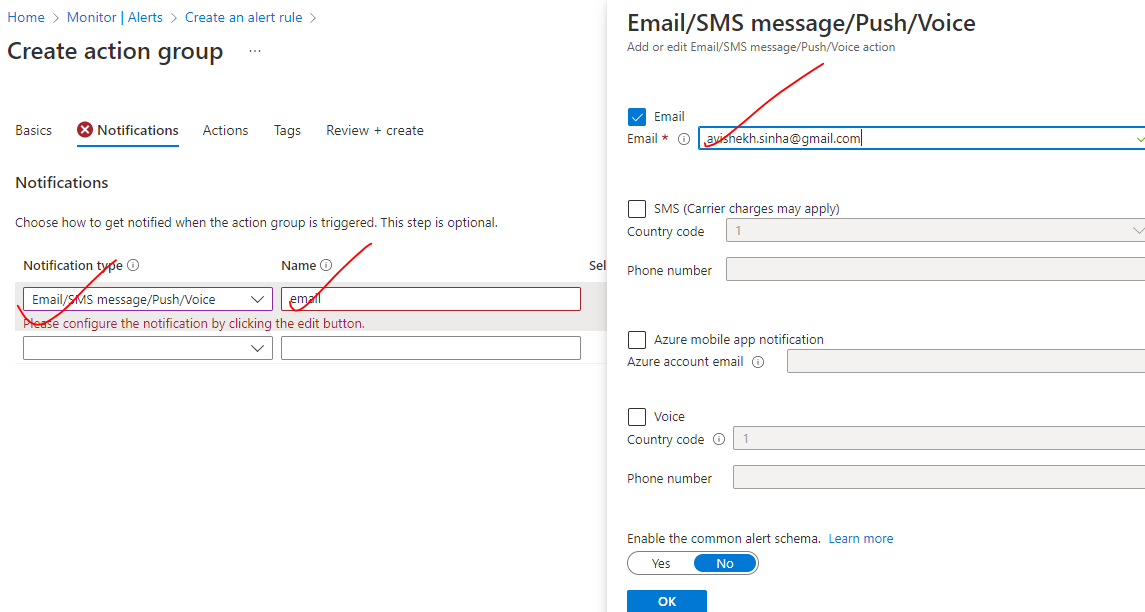
1. *STEP 4: BASED ON ADMIN OPERATIONS*



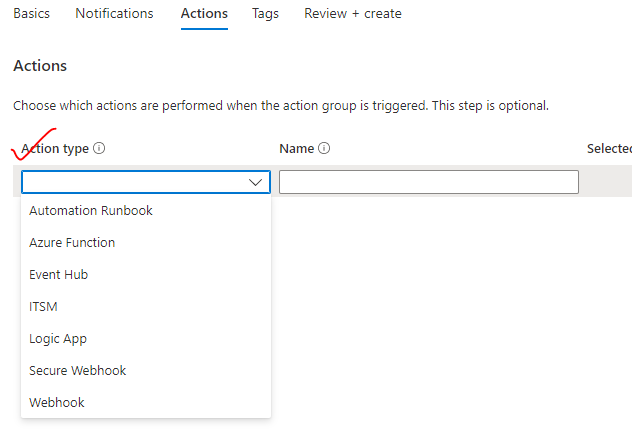


1. STEP 5: CREATE ACTION GROUP (ACTION TO BE PERFORMED

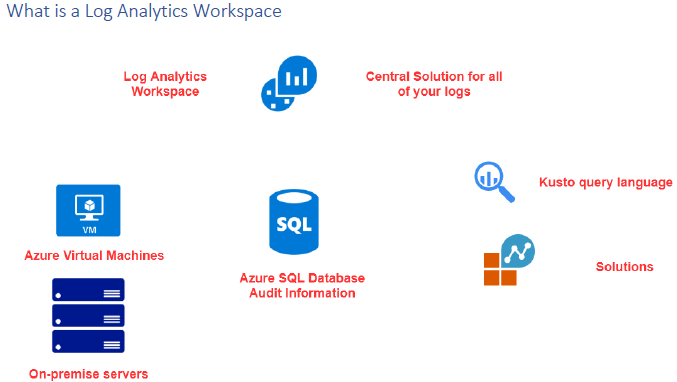




We can configure the notification to external system as well



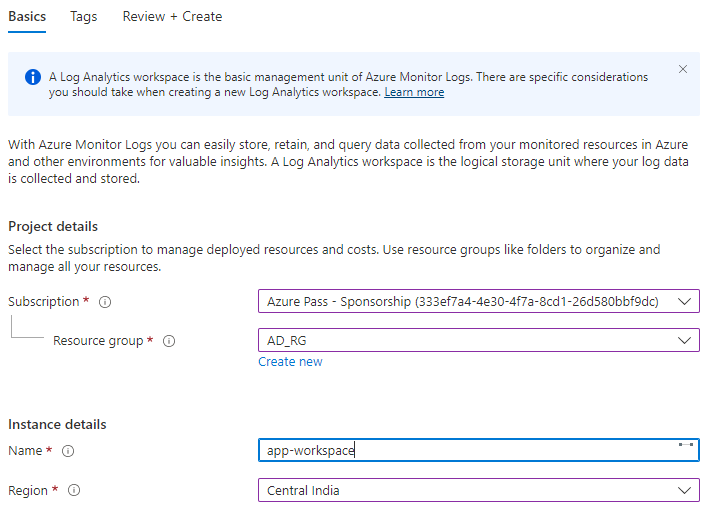
## LOG ANALYTICS WORKSPACE



* 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.



### CONNECTING A VM TO LOG ANALYTICS WORKSPACE

|  |  |
| --- | --- |
|  | * Log analytics workspace can be connect to Azure VM or on-premise server * To connect with Azure VM 🡪 Open the workspace 🡪 Workspace Data source 🡪 VM 🡪 Select the VM 🡪 Connect * This step will install an agent on the VM – which will start sending the data to the workspace. The agent is needed in both Azure VM and On-prem server |
| CONNECTING AZURE VM TO LOG ANALYTICS WORKSPACE | |
| CONNECTING ON PREM SERVER TO LOG ANALYTICS WORKSPACE  Let’s consider on Azure VM as on Prem server.  Step 1: Go the workspace 🡪 Agent Management🡪 The agent will be available as downloadable file.(as shown below)   * Let connect using RDP to the VM and copy the file in temp directory of the VM | |

