DEVOPS with MULTI-CLOUD
Practice Tasks

Institute Name : V Cube software solutions
Course **:** DevOps with Multi-Cloud
Batch **:** 30
Trainer **:** Krishna reddy sir

Prepared by **:** G.Bhavish
(MCD-AZ30-024)

TASK-21 :- Azure Monitor.

Date : 19/02/26

Objective :-

To monitor, analyze, and ensure the performance, availability, and security of Azure and hybrid resources by collecting and acting on telemetry data.

Azure Monitor :-

→ The Azure Monitor is a monitoring & observability service in microsoft azure that collects,analyzes and acts on telemetry data from azure resources on-premises systems and other cloud environments,

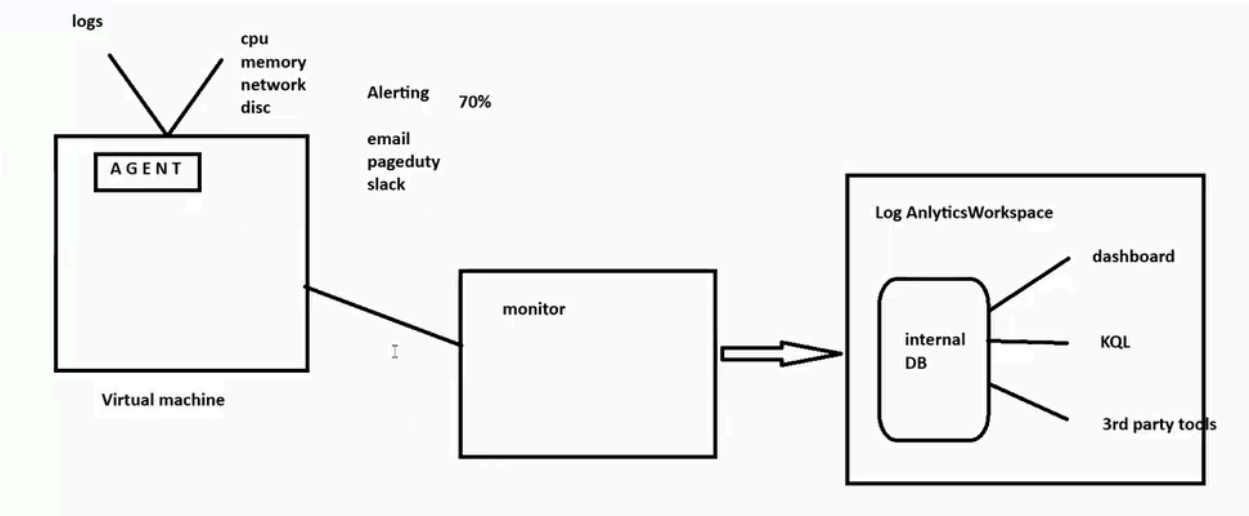
→ It helps us in :-

- Monitor performance
- Detect issues
- Set alerts
- Analyse logs
- Improve availability.

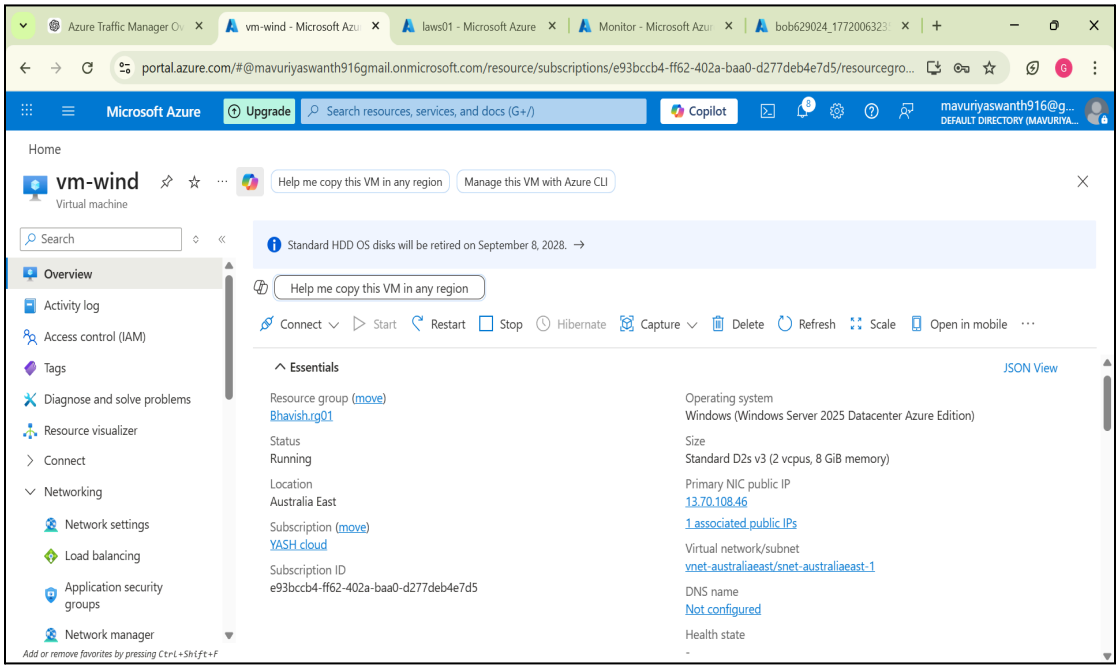
→ Types of data it mainly collects :-

- Metrics - numerical value
  eg: cpu%,memory usage.
- Logs - detailed records stored in log analytics workspace.

→ we monitor the machines to maintain the health status of the machines.



→ Create a Machine :-
rg01>vm-wind>Central india

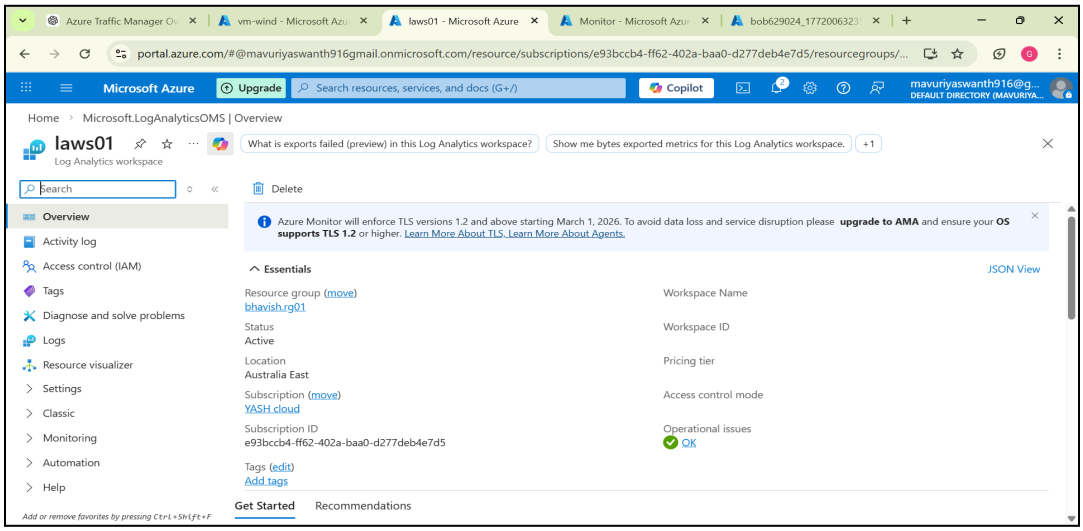


fig(1) windows machine is created.

→ create log analytics workspace

Search It>+create

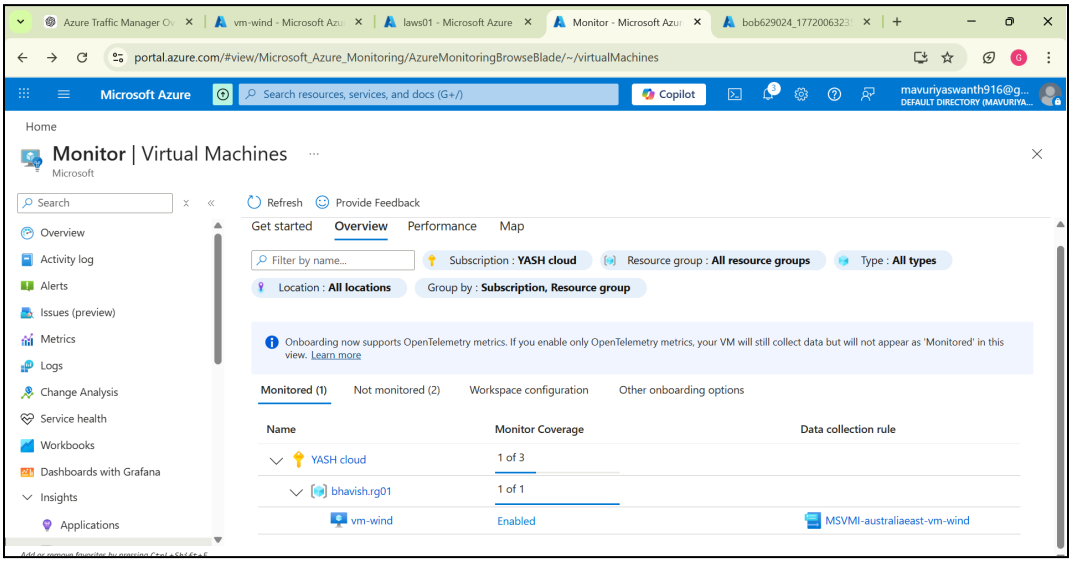
rog01>laws01>Central india.



fig(2) created log analytics workspace.

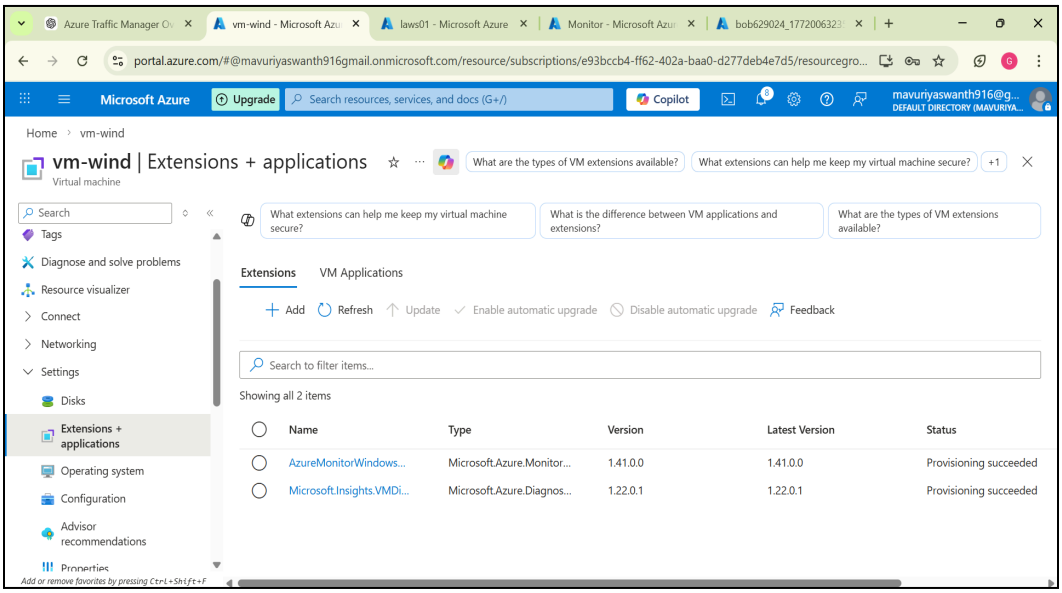
→ now if we goto the vm>extentions&applications we don’t find any agent.

→ now goto monitor and enable the vm-wind machine.



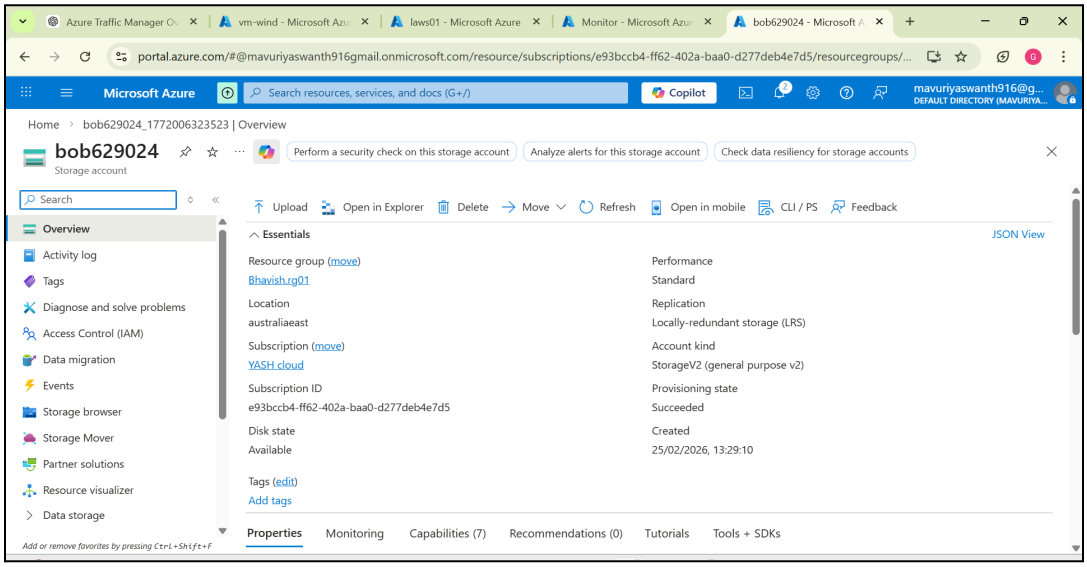
fig(3) enabled the monitor for the windows machine.

→ since we enabled the monitor on the machine the agent will be created automatically in the backend.



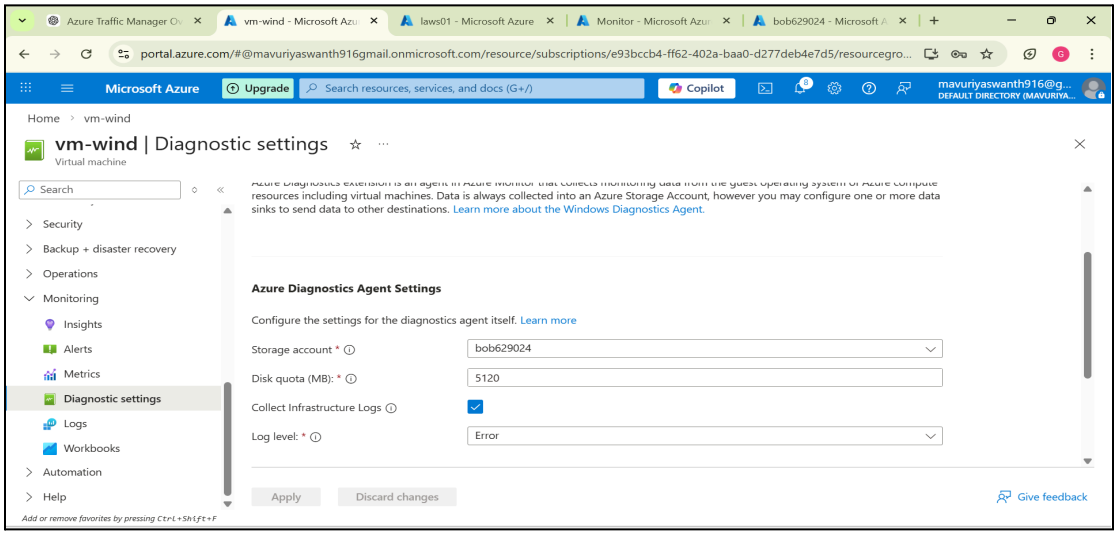
fig(4) the agent is automatically created in the backend.

→ Now create a storage account.



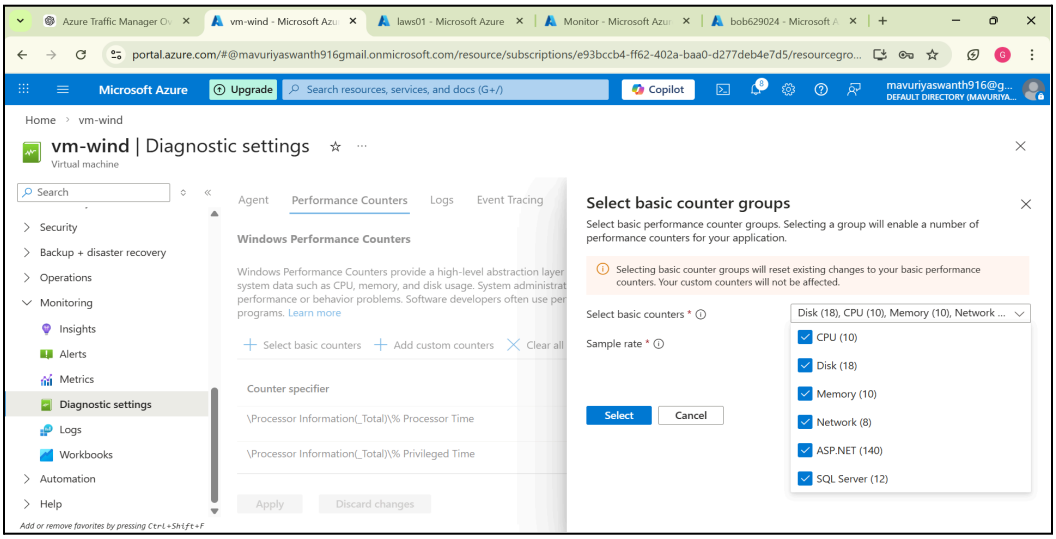
fig(5) created a storage account.

→ her, the agent will collect the data and send it to monitor and store the data in the log analytics workspace.
→ and in the log analytics work space we have an internal db, the logs are stored in the db.
→ now give this storage account in the diagnostic center.



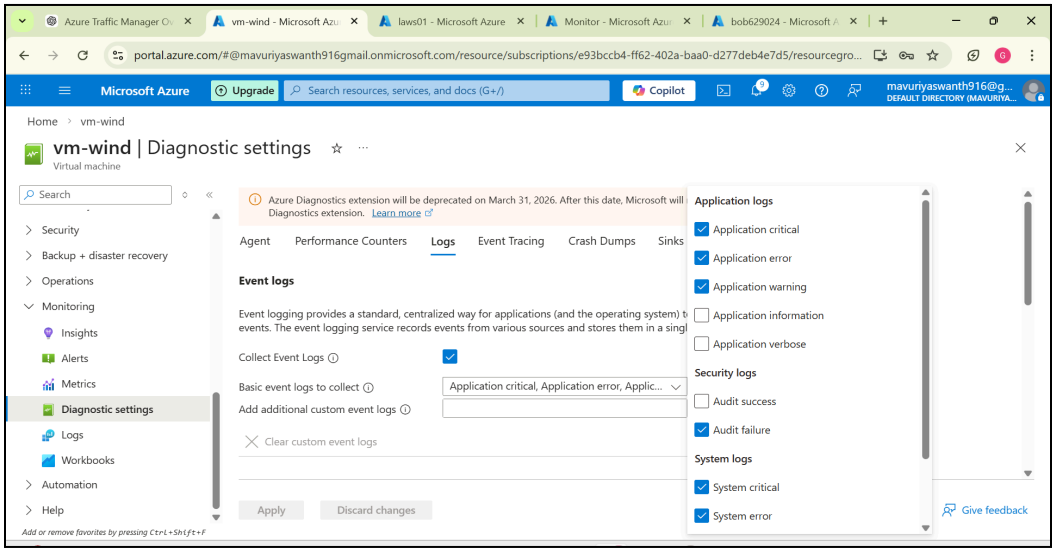
fig(6) selected the storage account in the diagnostics center.

→ now we need to select the basic counters to be monitored by the azure monitor.



fig(7) selecting counters which are to be monitored.

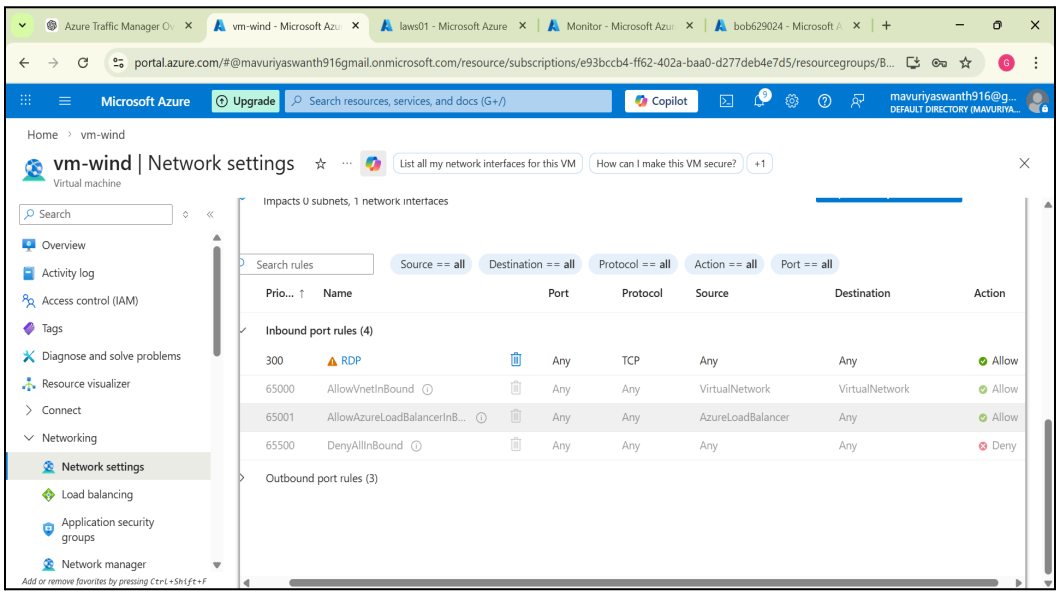
→ now we need to also select the logs, it contains all the records from various sources.



fig(8) selecting the logs for analyzing the log records.

→ Now goto the nsg rules, change the inbound RDP rule.

S : any, D : any, service : custom, Dport : *any, P : TCP.



fig(9) changed nsg rules.

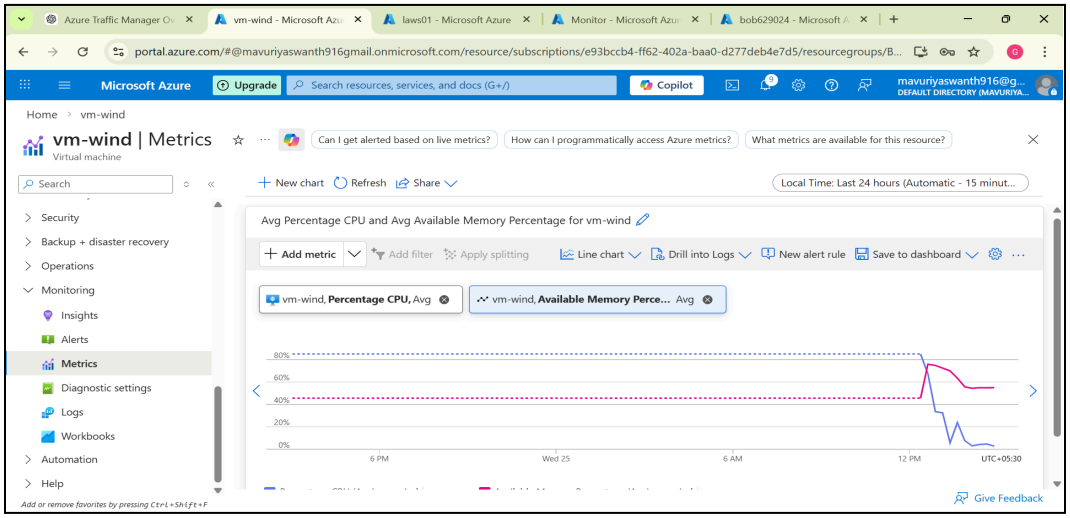
→ so that any traffic will flow to the machine.

→ Now select metrics.

vm-wind>monitoring>metrics.

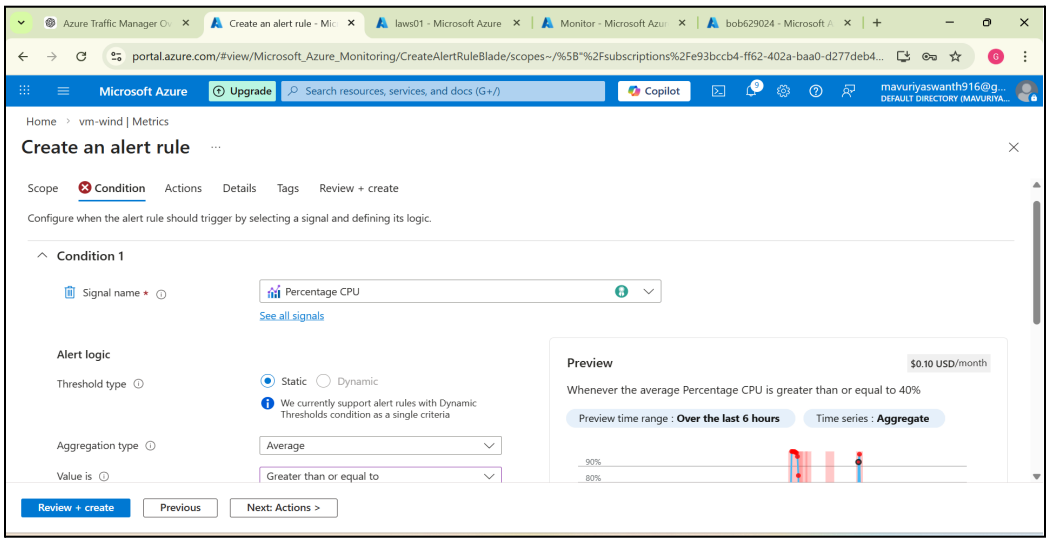
Metric 1 - %cpu

Metric 2 - available memory %.

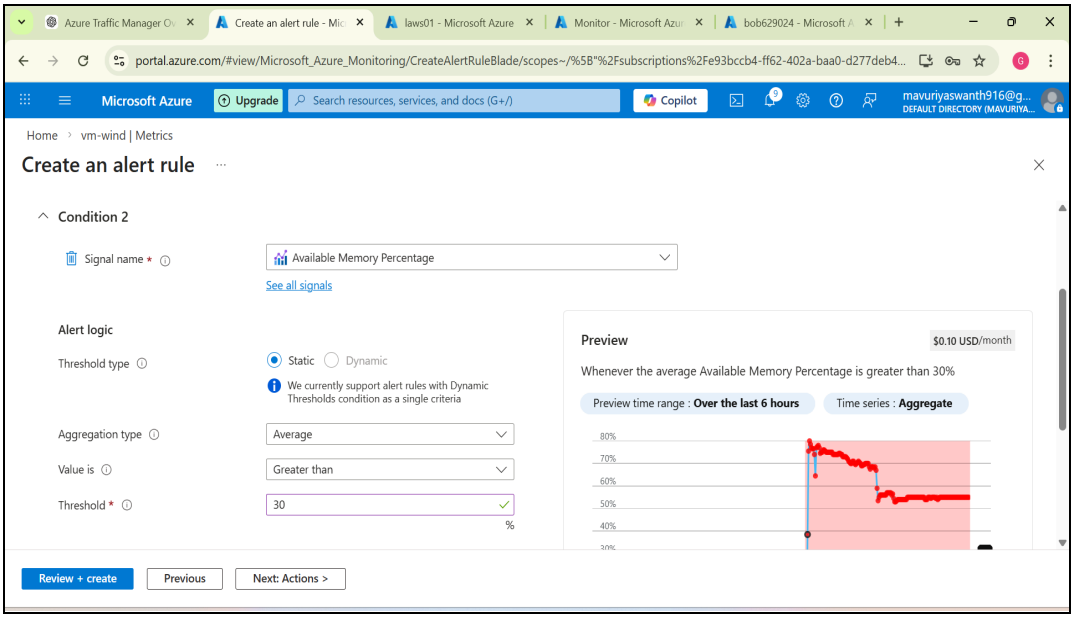


fig(10) selected two metrics so that the agent will collect data.

→ Now write the new alert rules. We will have conditions for the metrics selected, so that if the value is more than it is mentioned in the condition,it will trigger the alert system.



fig(11) condition1 in the alert rule.



fig(12) condition 2 in the alert rule.

→ Now in the actions, create an action group. So that when the alert rule is triggered then these are actions needed to perform.

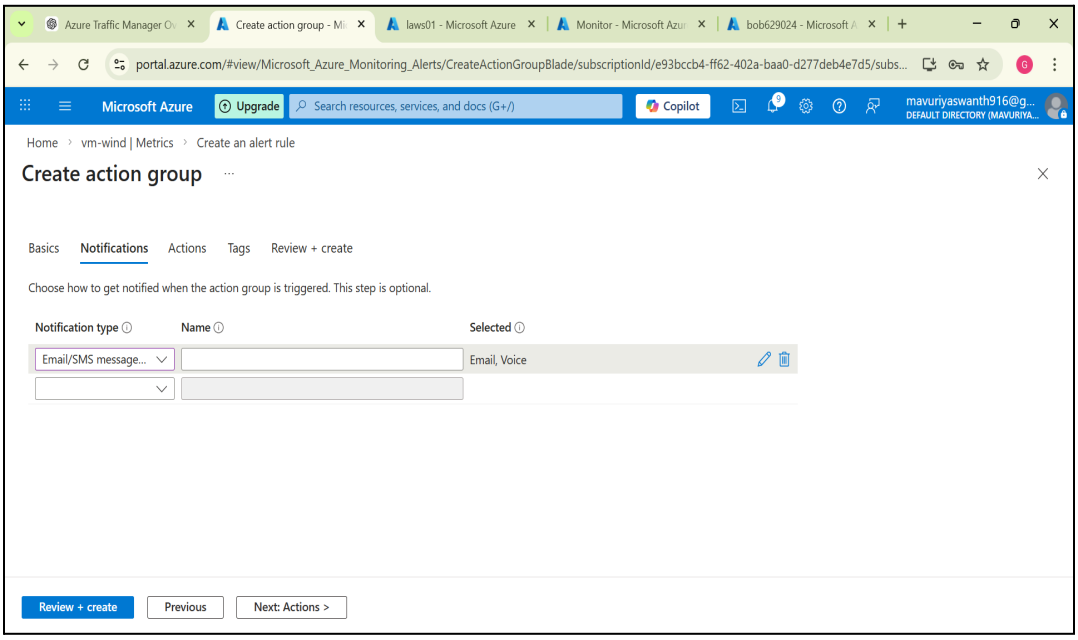
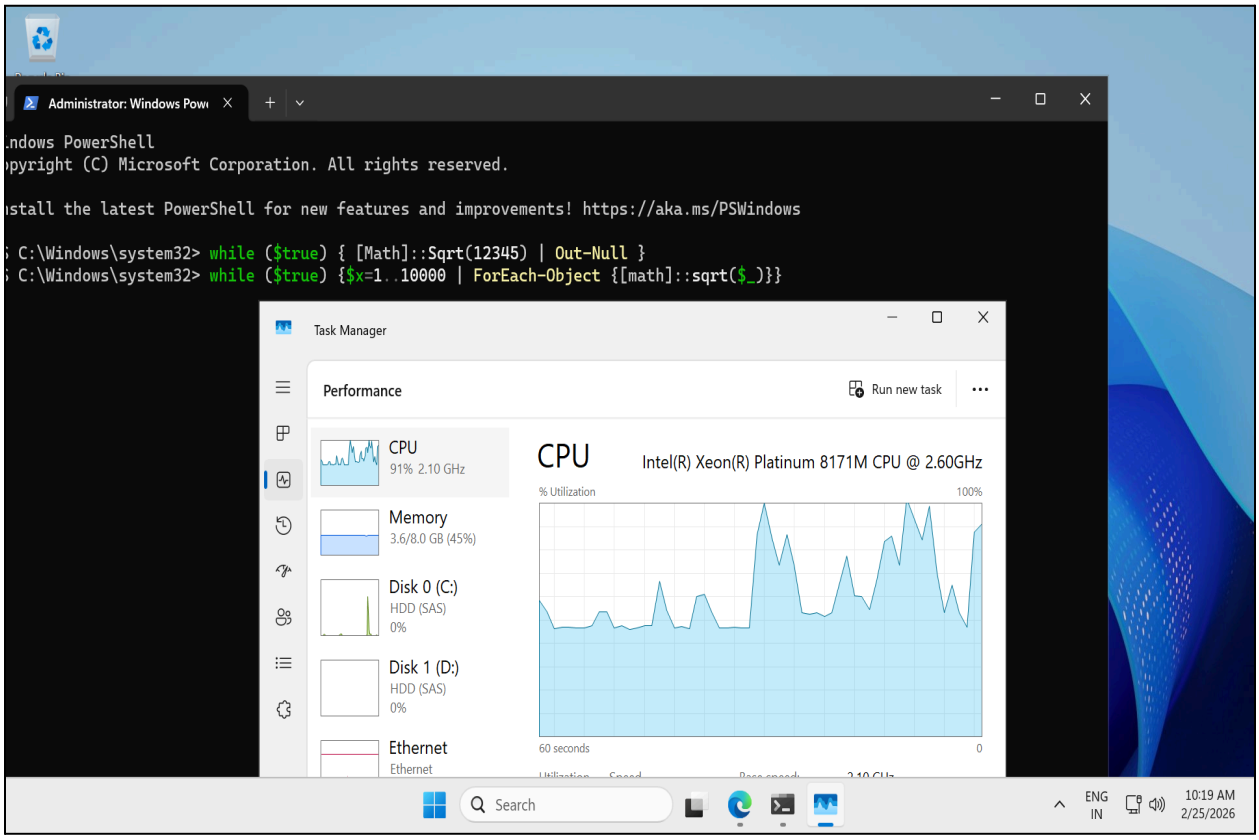


Fig (13) created an action group with email & voice.

→ Now login to the windows machine and apply the stress on the CPU.
→ To apply stress :- we can use the in-build stress in windows.

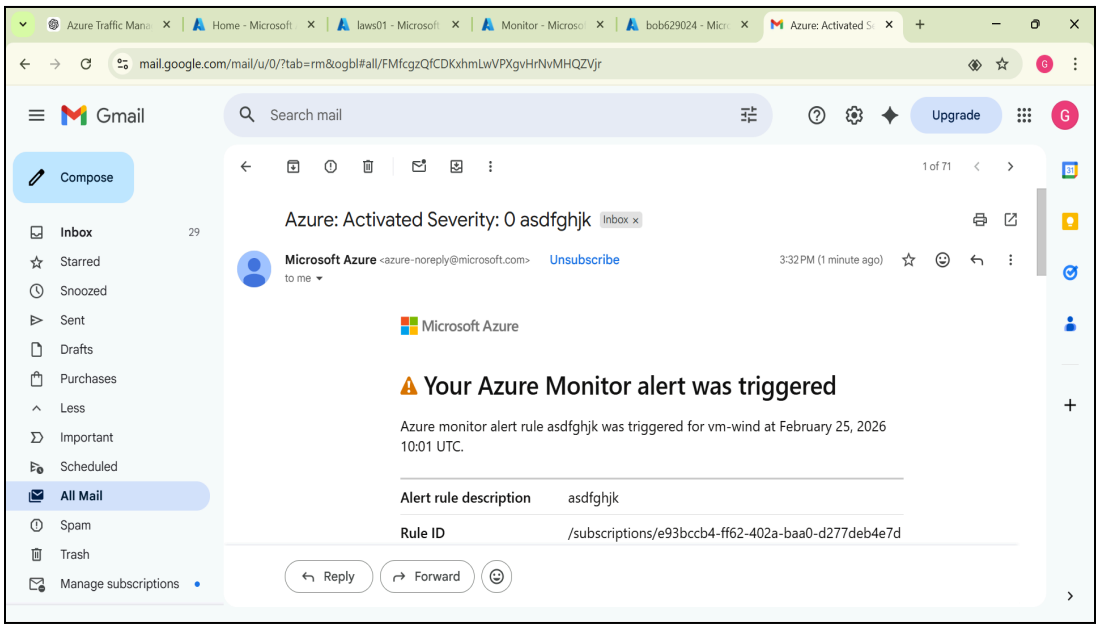
- Goto windows powershell and run this command.
  - while ($true) { [Math]::Sqrt(12345) | Out-Null }

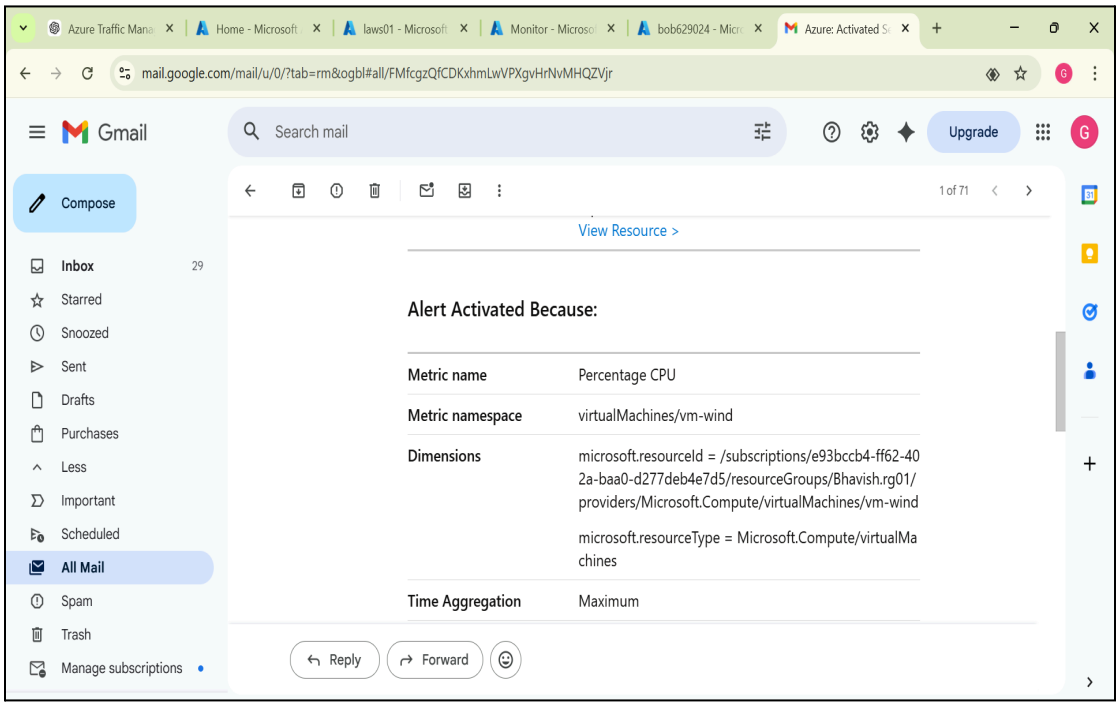
→ now the cpu % will be increased >> the alert rule will be triggered >> the defined action is performed.

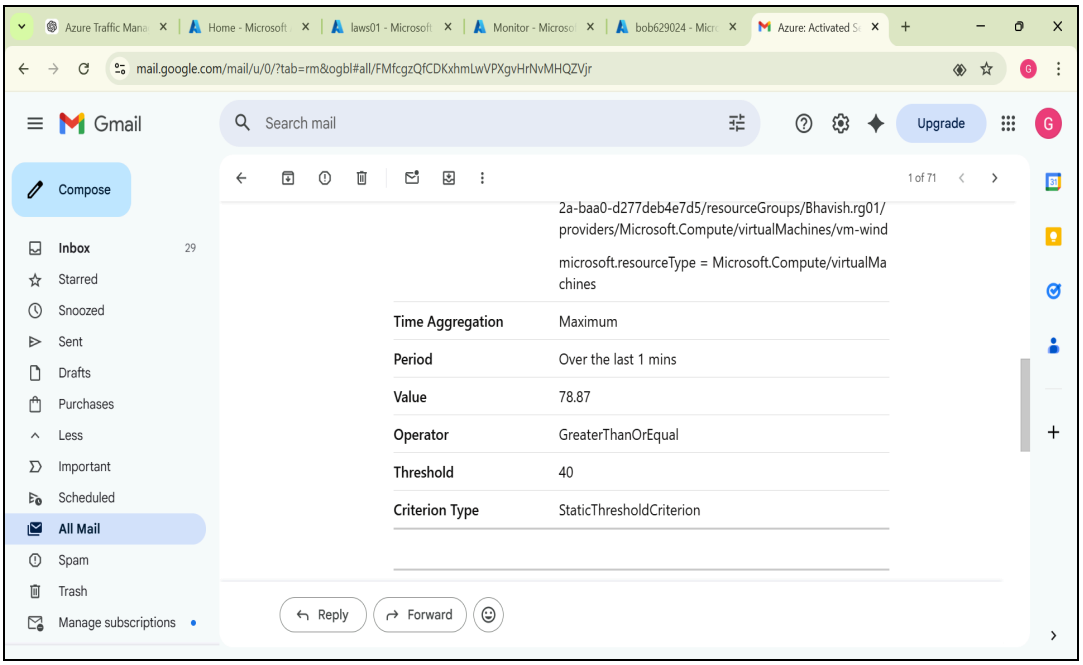


fig(14) the command is executed and the cpu% is increased.

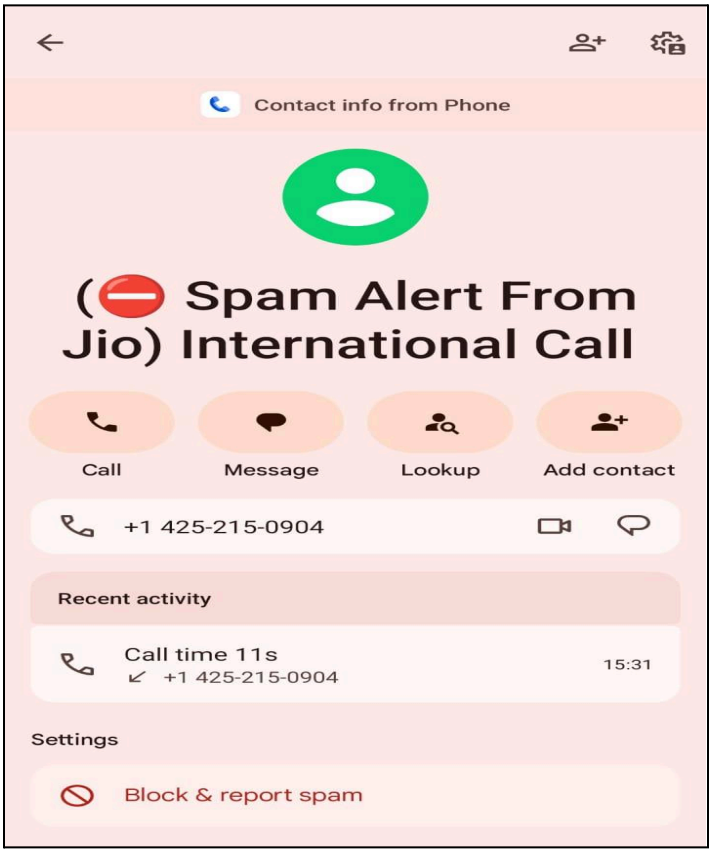
→ Since the CPU% is increased the alert action email and the voice will be performed.







fig(15,16,17) the email action which is sent to mail.



fig(18) the voice action.

→ like this we can monitor the machines using the azure monitor.
→ if there are multiple vm’s then we can monitor them by hub&spoke architecture and vnet peering.
→ generally these all are native tools of the azure. But companies use 3rd party tools like Grafana and Prometheus.