

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,

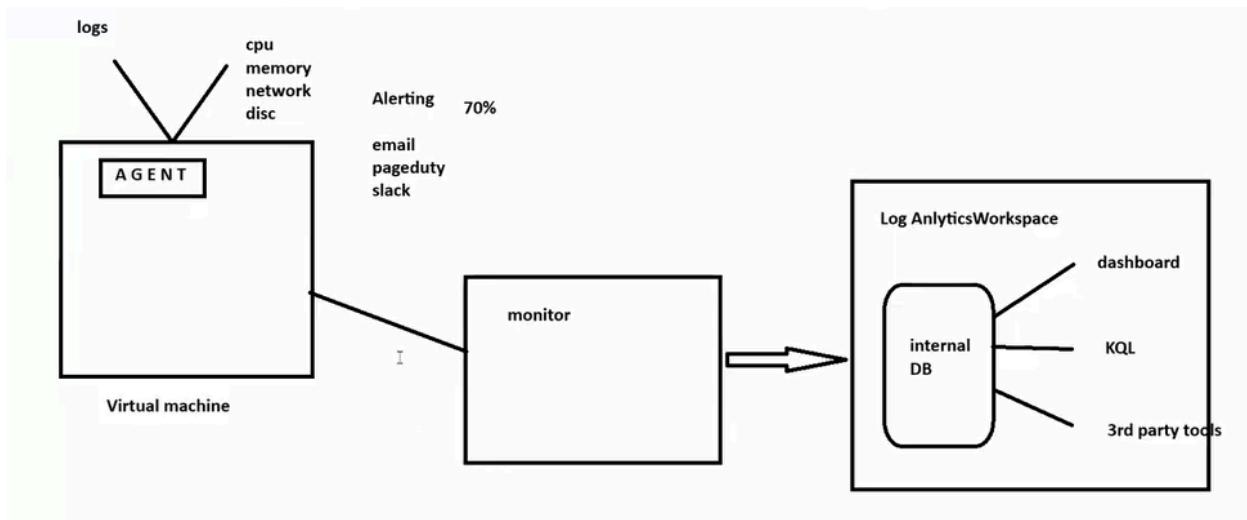
→ It helps us in :-

- 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

Essentials	Value
Resource group (move)	Bhavish.rg01
Status	Running
Location	Australia East
Subscription (move)	YASH.cloud
Subscription ID	e93bccb4-ff62-402a-baa0-d277deb4e7d5
Operating system	Windows (Windows Server 2025 Datacenter Azure Edition)
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Primary NIC public IP	13.70.108.46
Associated public IPs	1 associated public IPs
Virtual network/subnet	vnet-australiaeast/snet-australiaeast-1
DNS name	Not configured
Health state	-

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.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Azure Traffic Manager', 'vm-wind - Microsoft Azure', 'laws01 - Microsoft Azure', 'Monitor - Microsoft Azure', and 'bob629024_1772006323523'. The main title is 'vm-wind | Extensions + applications'. On the left, a sidebar lists 'Home', 'vm-wind', 'Extensions + applications' (which is selected), 'Operating system', 'Configuration', 'Advisor recommendations', and 'Properties'. The main content area has tabs for 'Extensions' and 'VM Applications'. Under 'Extensions', there are buttons for '+ Add', 'Refresh', 'Update', 'Enable automatic upgrade' (unchecked), and 'Disable automatic upgrade' (checked). A search bar says 'Search to filter items...'. Below it, a table lists extensions: Name, Type, Version, Latest Version, and Status. Two entries are shown:

Name	Type	Version	Latest Version	Status
AzureMonitorWindows...	Microsoft.Azure.Monitor...	1.41.0.0	1.41.0.0	Provisioning succeeded
Microsoft.Insights.VMDi...	Microsoft.Azure.Diagnostics...	1.22.0.1	1.22.0.1	Provisioning succeeded

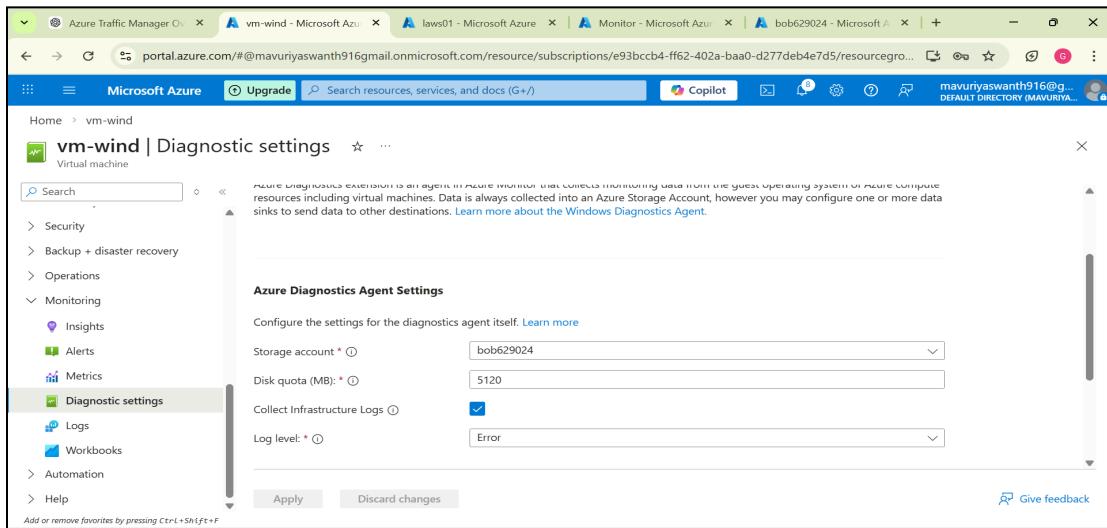
fig(4) the agent is automatically created in the backend.

→ Now create a storage account.

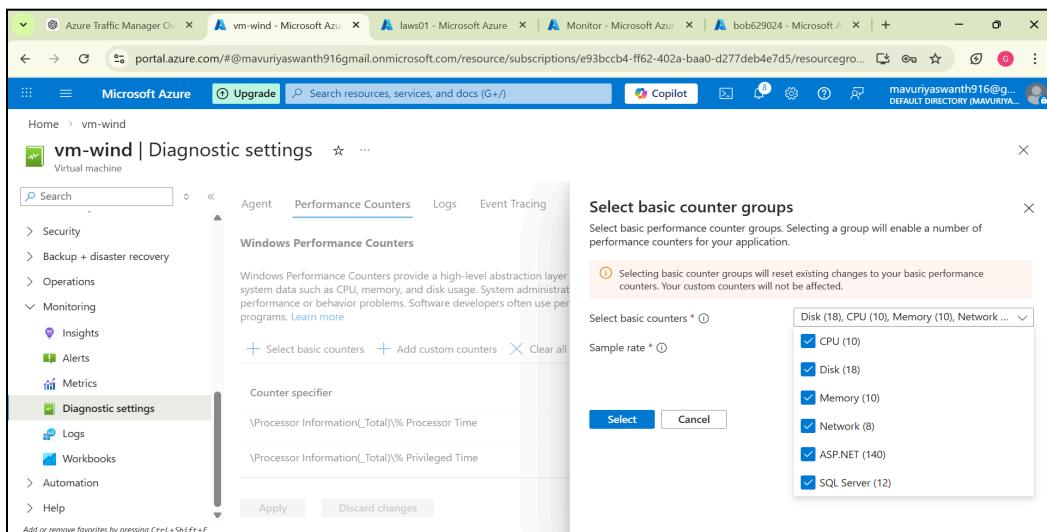
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for 'Azure Traffic Manager', 'vm-wind - Microsoft Azure', 'laws01 - Microsoft Azure', 'Monitor - Microsoft Azure', and 'bob629024 - Microsoft Azure'. The main title is 'bob629024 | Overview'. On the left, a sidebar lists 'Home', 'bob629024', 'Storage account' (which is selected), 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage browser', 'Storage Mover', 'Partner solutions', 'Resource visualizer', and 'Data storage'. The main content area has tabs for 'Upload', 'Open in Explorer', 'Delete', 'Move', 'Refresh', 'Open in mobile', 'CLI / PS', and 'Feedback'. The 'Overview' section displays details: Resource group (move) to 'Bhavishyng01', Location to 'australiaeast', Subscription (move) to 'YASH cloud', Subscription ID to 'e93bccb4-ff62-402a-baa0-d277deb4e7d5', Disk state to 'Available', and Tags (edit) and Add tags options. At the bottom, tabs include 'Properties' (selected), 'Monitoring', 'Capabilities (7)', 'Recommendations (0)', 'Tutorials', and 'Tools + SDKs'. A note at the bottom left says 'Add or remove favorites by pressing Ctrl+Shift+F'.

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.

Azure Diagnostics extension will be deprecated on March 31, 2026. After this date, Microsoft will stop supporting the Azure Diagnostics extension. [Learn more](#)

Agent Performance Counters **Logs** Event Tracing Crash Dumps Sinks

Event logs

Event logging provides a standard, centralized way for applications (and the operating system) to log events. The event logging service records events from various sources and stores them in a single log file.

Collect Event Logs

Basic event logs to collect Application critical, Application error, Appl...

Add additional custom event logs

Clear custom event logs

Apply Discard changes

Application logs

Application critical
 Application error
 Application warning
 Application information
 Application verbose

Security logs

Audit success
 Audit failure

System logs

System critical
 System error

Give feedback

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.

Impacts U subnets, 1 network interfaces

Search rules Source == all Destination == all Protocol == all Action == all Port == all

Prio...	Name	Port	Protocol	Source	Destination	Action
300	RDP	Any	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Outbound port rules (3)

fig(9) changed nsg rules.

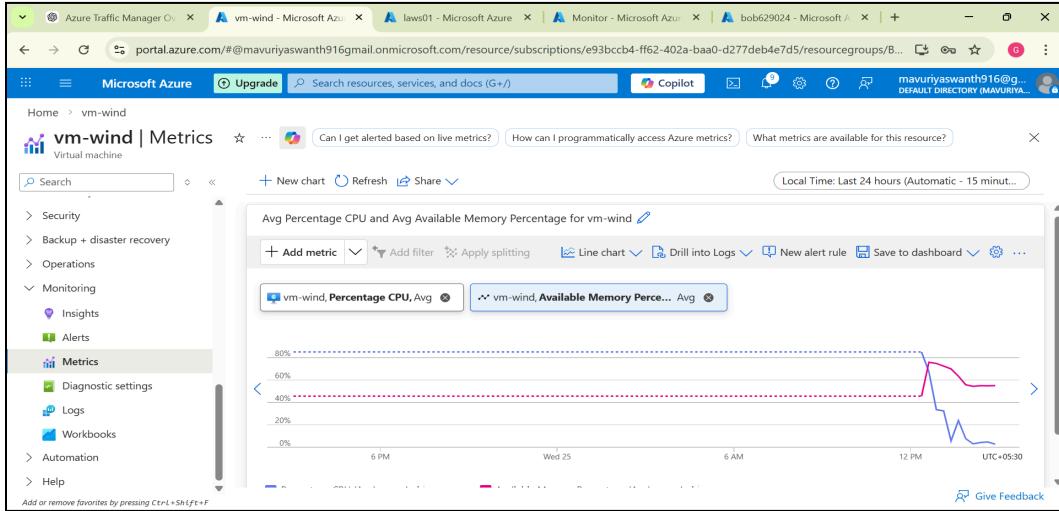
→ so that any traffic will flow to the machine.

→ Now select metrics.

vm-wind>monitoring>metrics.

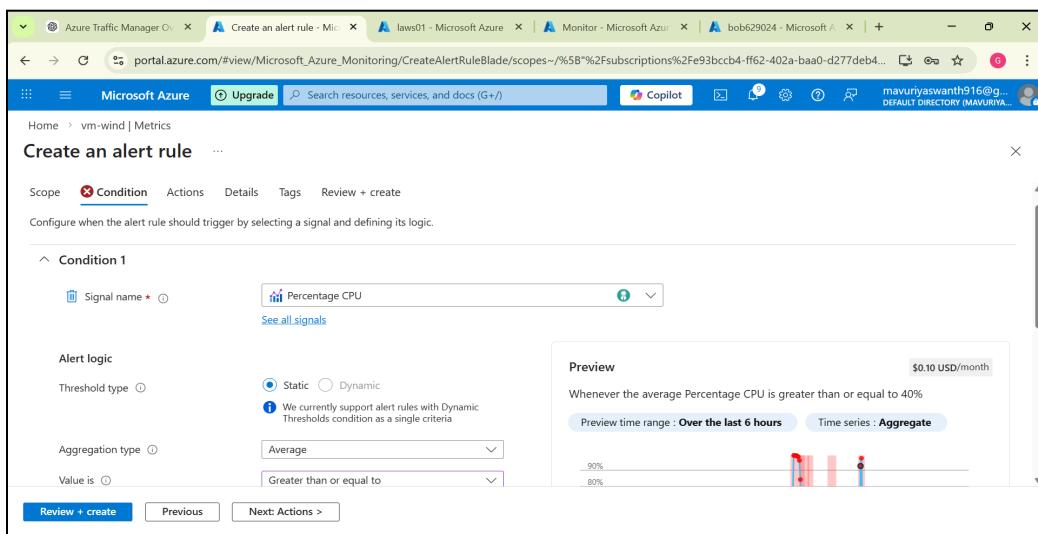
Metric 1 - %cpu

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.

The screenshot shows the 'Create an alert rule' interface in the Azure portal. The 'Condition 2' section is active. The signal selected is 'Available Memory Percentage'. The threshold type is 'Static' (selected), with a value of '30'. The aggregation type is 'Average'. The preview chart shows a red line representing memory usage over time, with a vertical blue line at 30% indicating the threshold. The chart has a tooltip '\$0.10 USD/month'.

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.

The screenshot shows the 'Create action group' interface in the Azure portal. The 'Notifications' tab is selected. The table shows two rows under 'Notification type': 'Email/SMS message...' and another row below it. The 'Selected' column for both rows shows 'Email, Voice'.

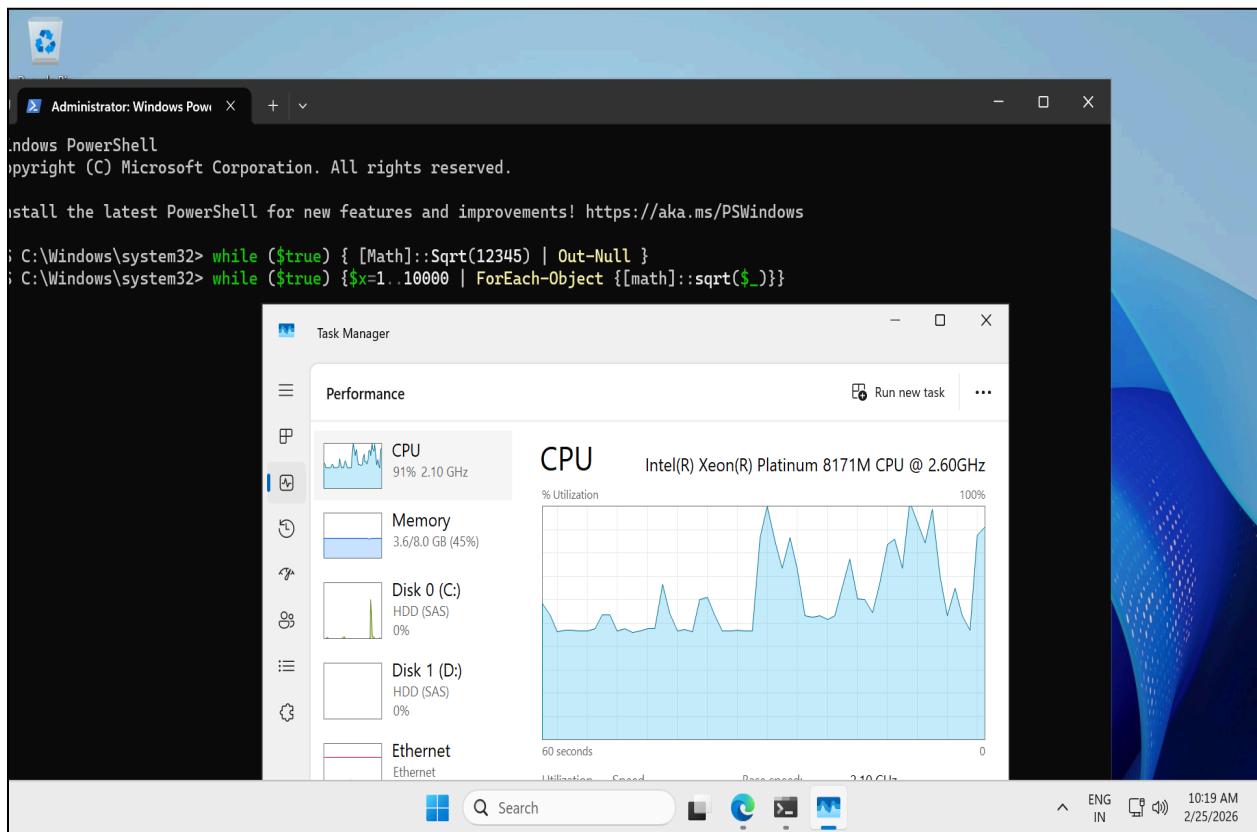
Fig (13) created an action group with email & voice.

→ 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.

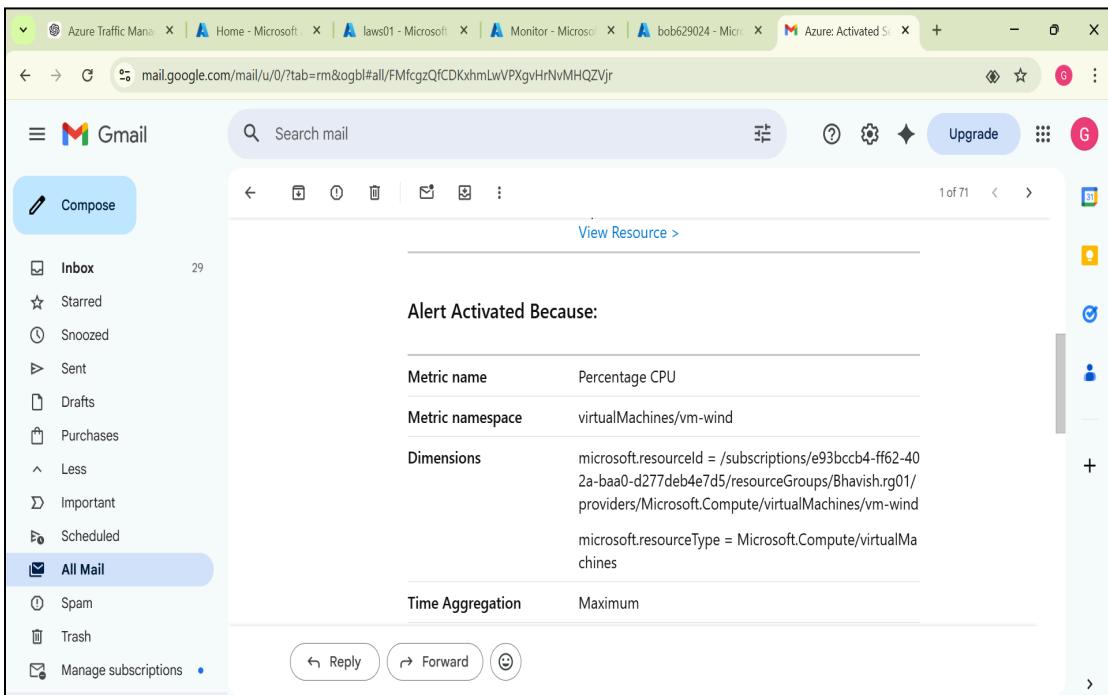
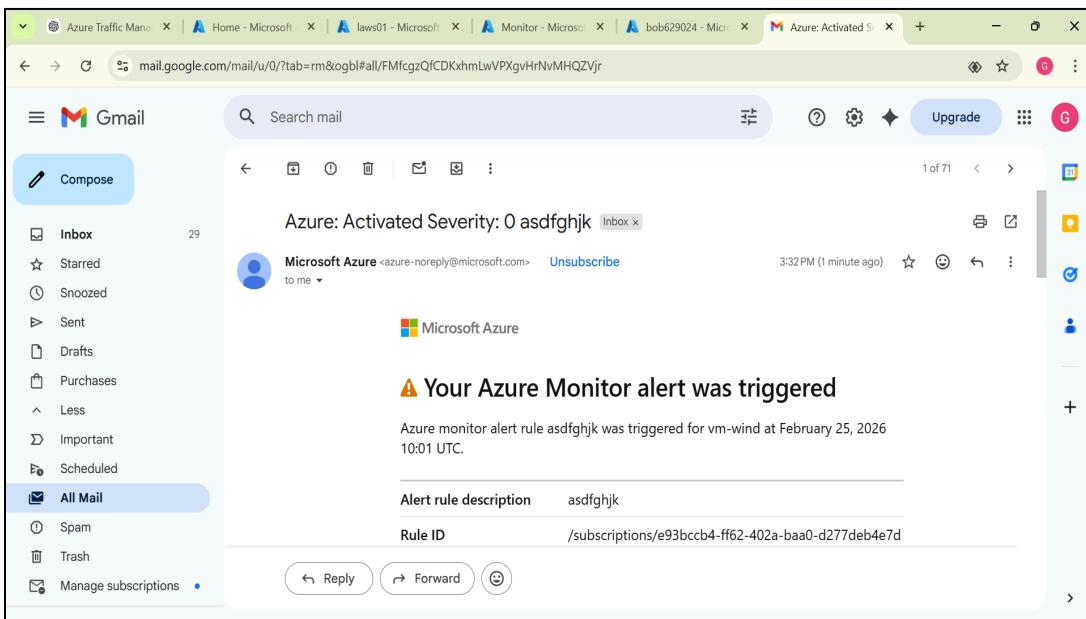
- Goto windows powershell and run this command.
 - `while ($true) { [Math]::Sqrt(12345) | Out-Null }`

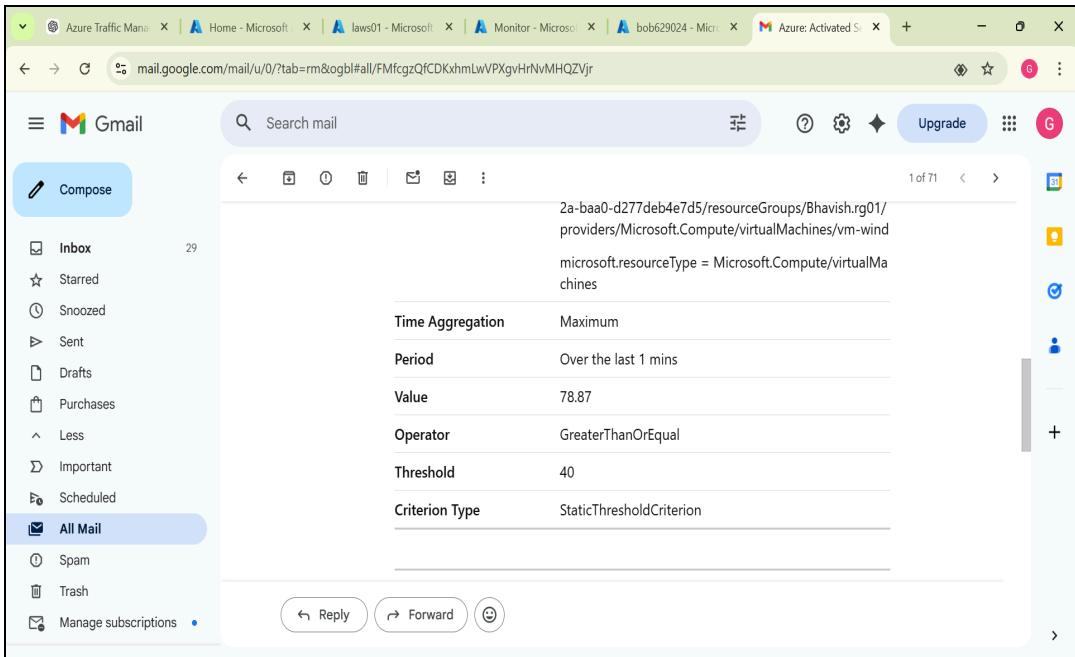
→ now the cpu % will be increased >> the alert rule will be triggered >> the defined action is performed.



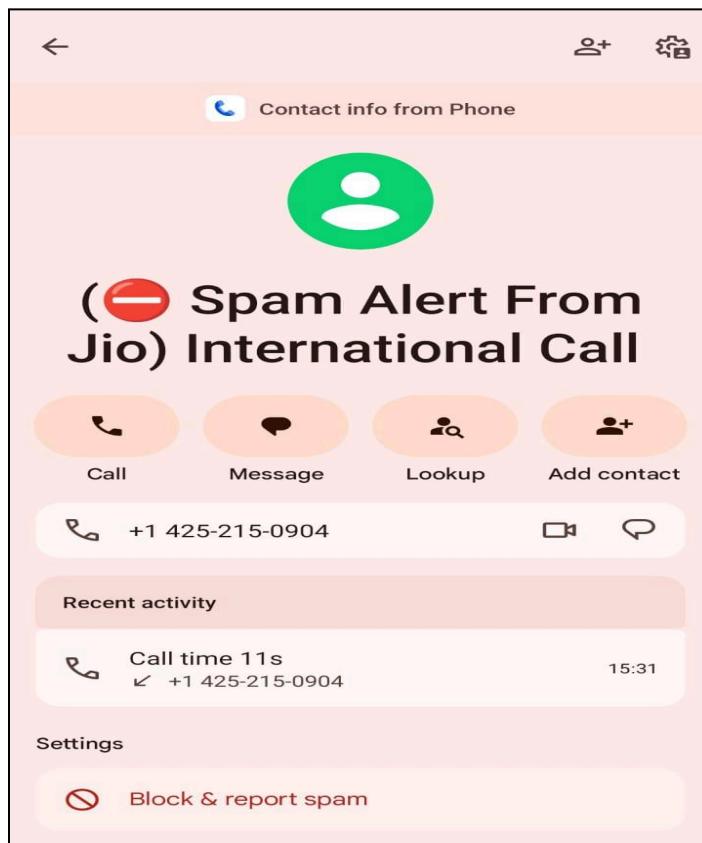
fig(14) the command is executed and the cpu% is increased.

→ 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.

