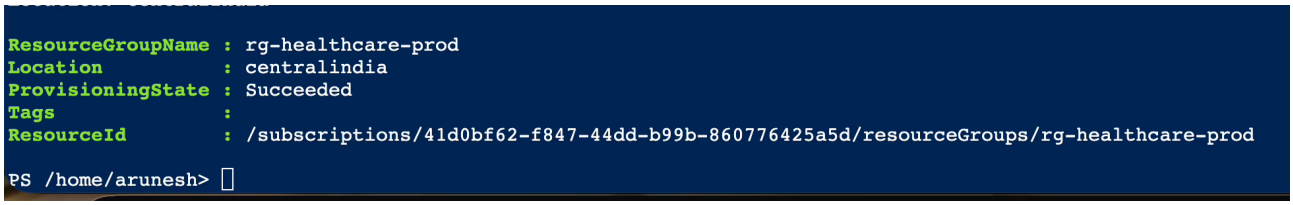
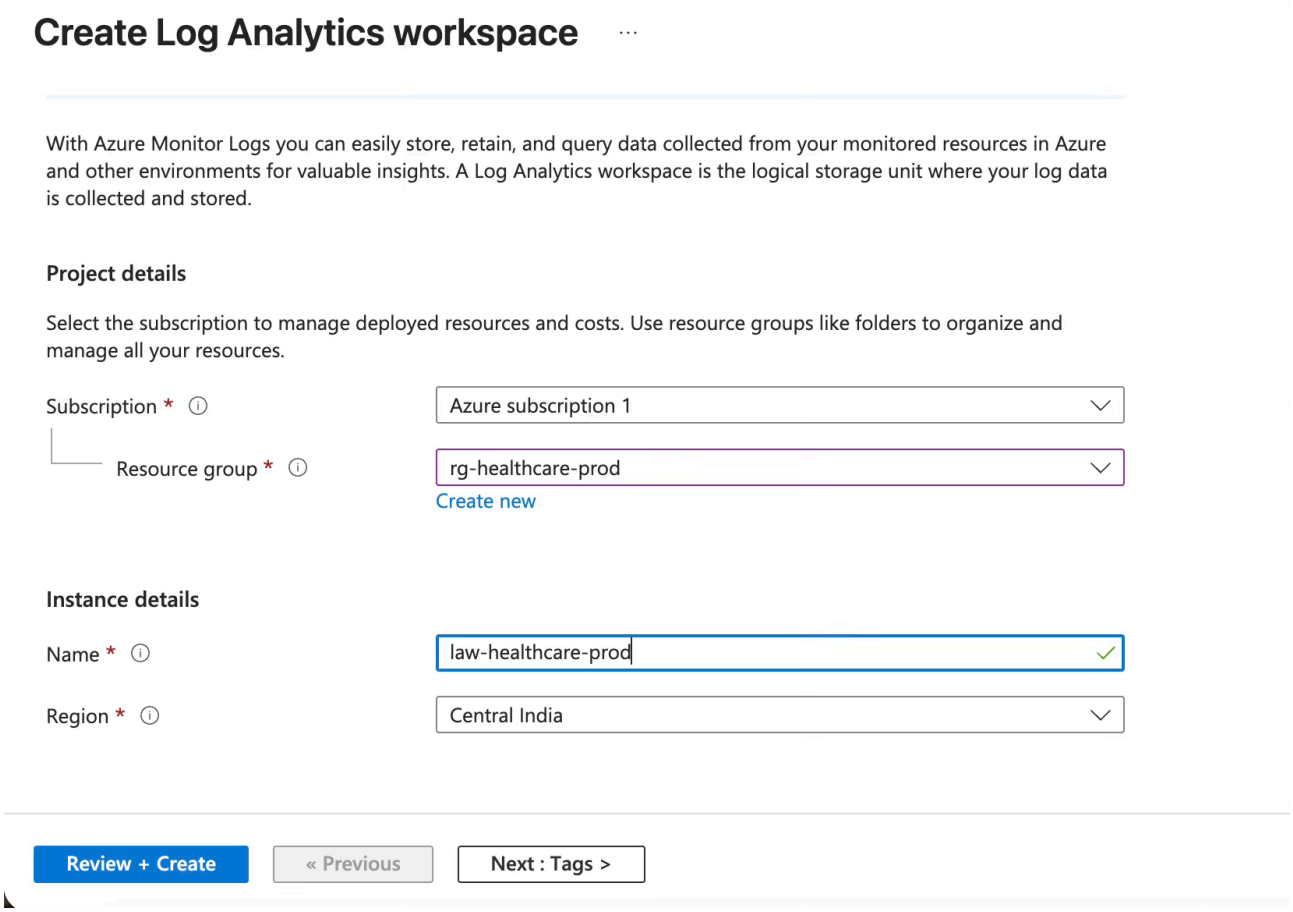
Project: Healthcare Claims Processing & Failure Detection Platform

Step-1: Created ResourceGroup Name: rg-healthcare-prod.



Step-2: Created Log analytics workspace name: law-healthcare-prod.



Basics Tags **Review + Create**

Log Analytics workspace
by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	rg-healthcare-prod
Name	law-healthcare-prod
Region	Central India

Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. are available on the Azure Monitor pricing page. You can change to a different pricing tier after t created. Learn more about Log Analytics pricing models.

Create « Previous Download a template for automation

Step-3: Created Virtual Network name given: vnet-healthcare-prod.

Basics Security IP addresses Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * rg-healthcare-prod

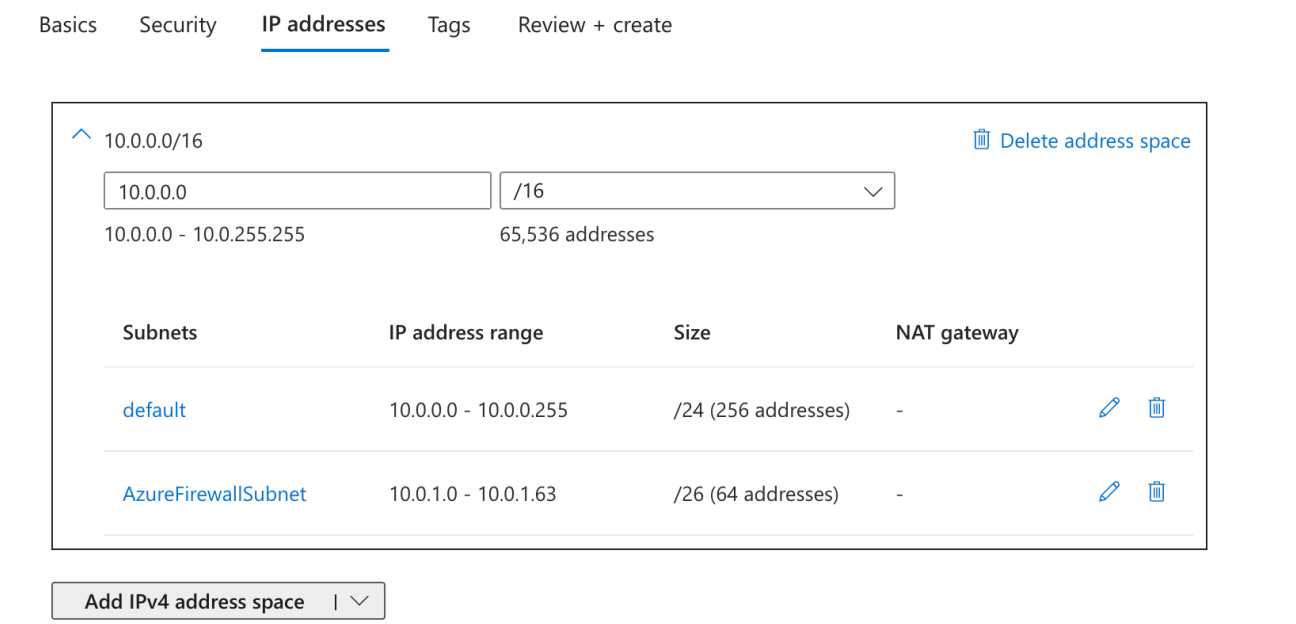
Create new

Instance details

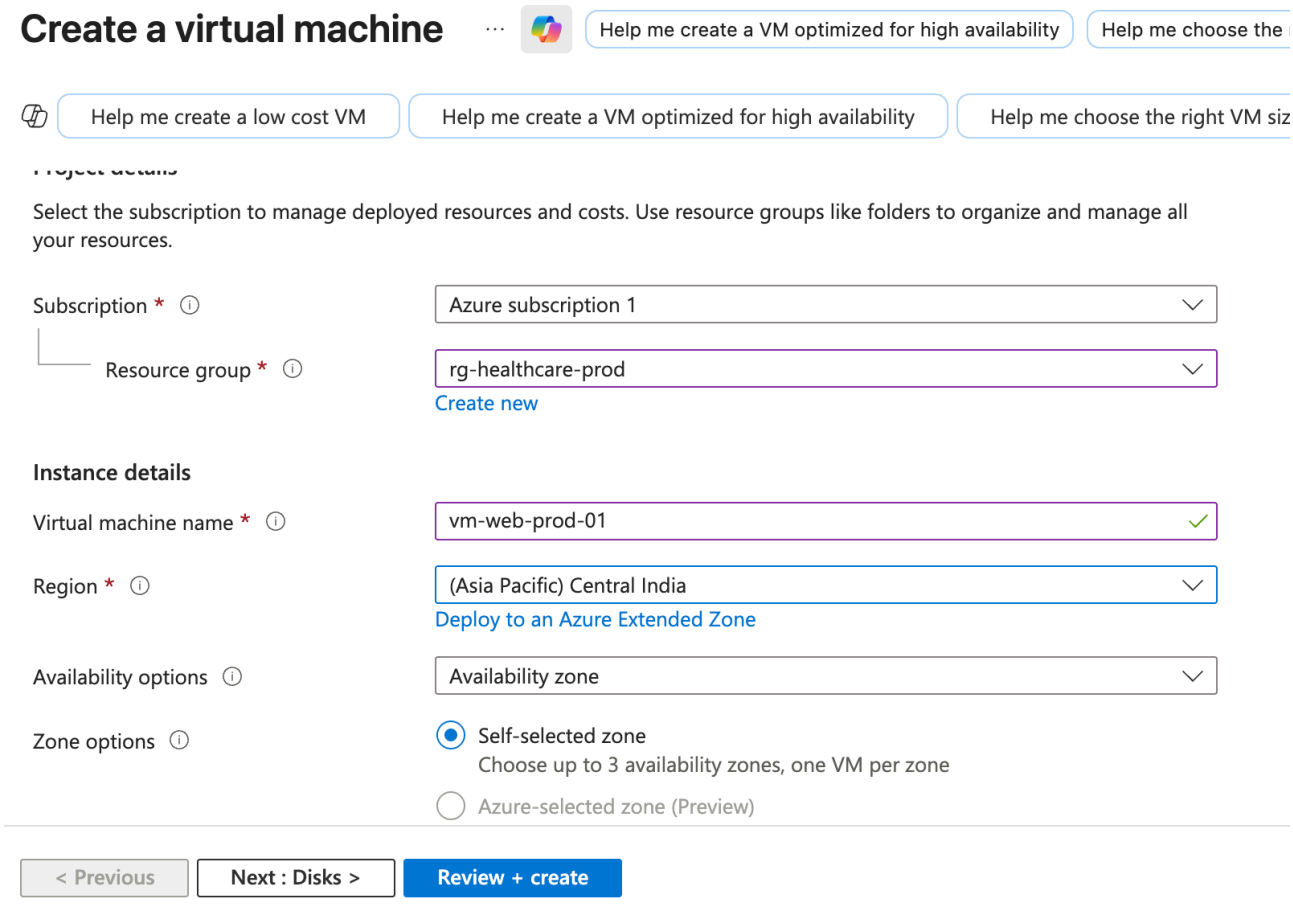
Virtual network name * vnet-healthcare-prod

Region * (Asia Pacific) Central India

Previous Next **Review + create**



Step-4: Created a Web VM name given: vm-web-prod-01.



Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for

Availability zone * ⓘ: Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type ⓘ: Trusted launch virtual machines

Configure security features

Image * ⓘ: Ubuntu Server 24.04 LTS - x64 Gen2 (free services eligible)

See all images | Configure VM generation

VM architecture ⓘ: ○ Arm64 ◉ x64

Run with Azure Spot discount ⓘ: ☐

You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. Learn more

< Previous | Next : Disks > | Review + create

OS disk

OS disk size ⓘ: Image default (30 GiB)

OS disk type * ⓘ: Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ⓘ: ☑

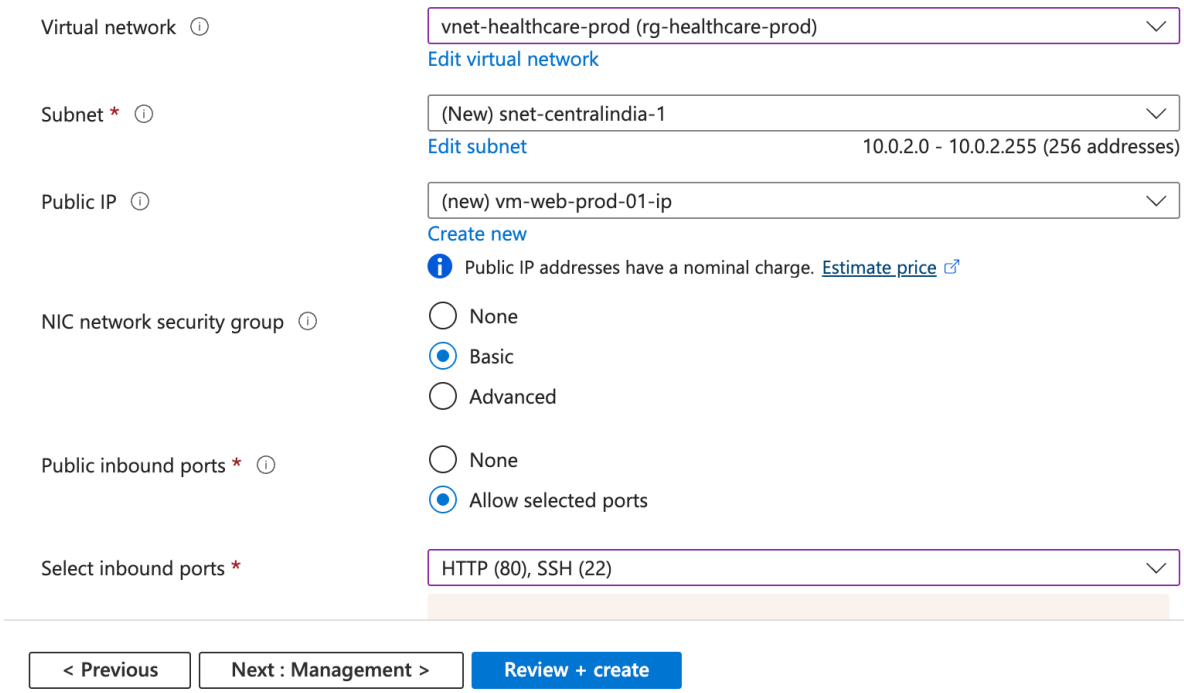
Key management ⓘ: Platform-managed key

Enable Ultra Disk compatibility ⓘ: ☐

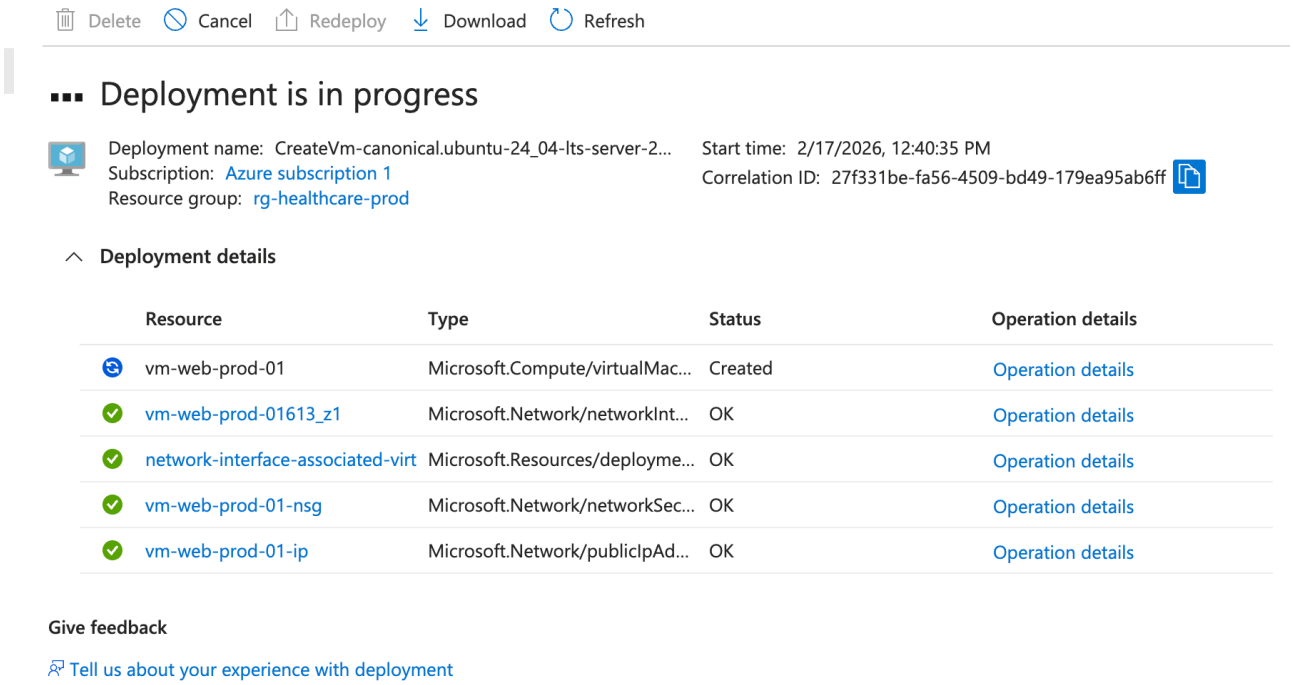
Data disks for vm-web-prod-01

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a

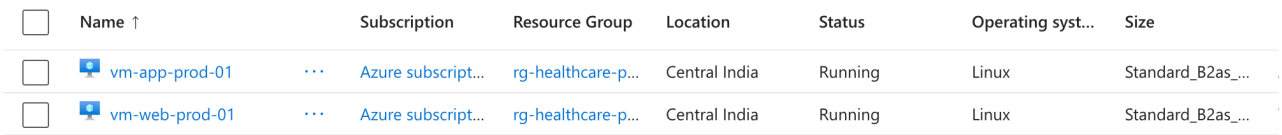
< Previous | Next : Networking > | Review + create



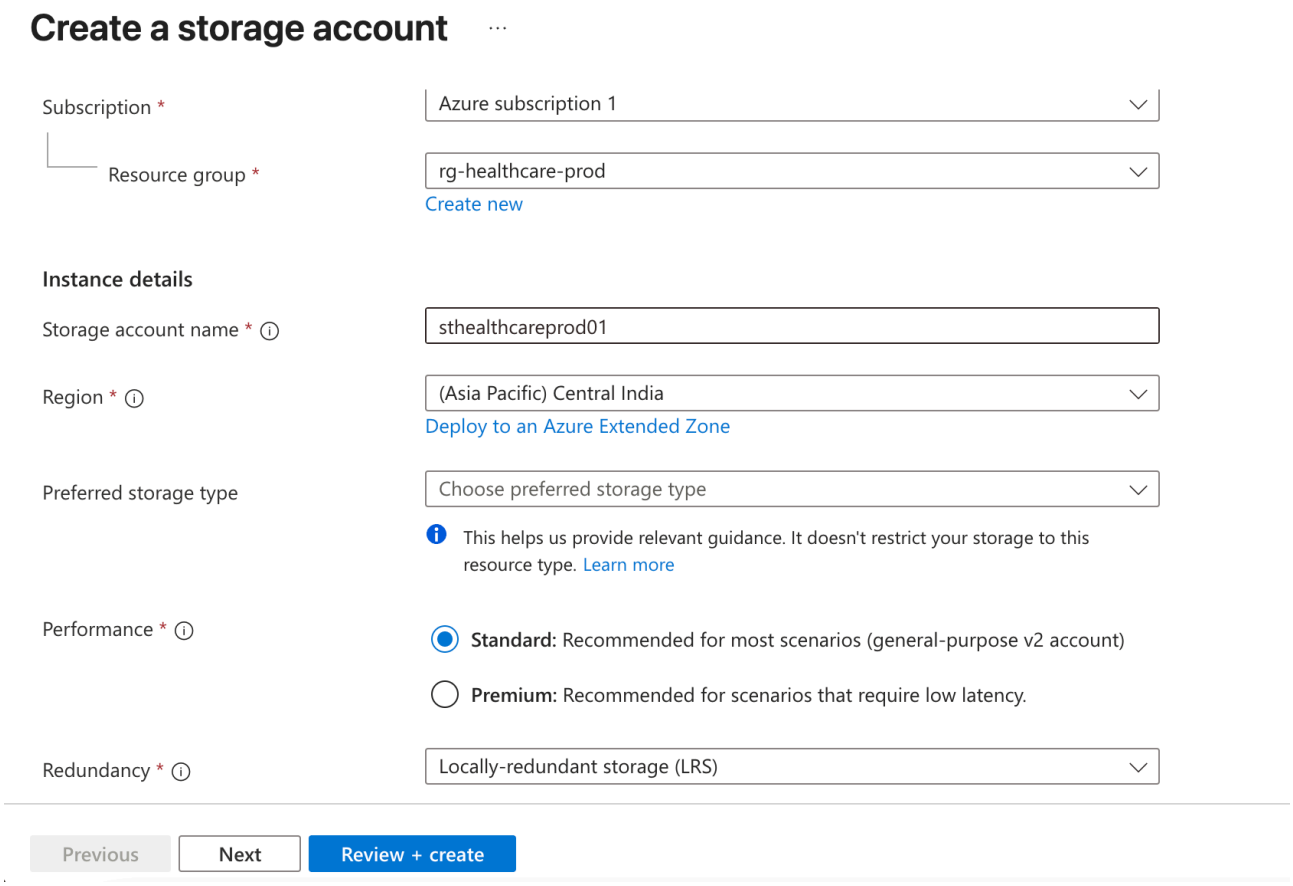
Management Tab - Keep default



Step-5: Created App vm as well snapshot below for the reference:



Step-6: Created a storage name given: sthealthcareprod01.



View automation template

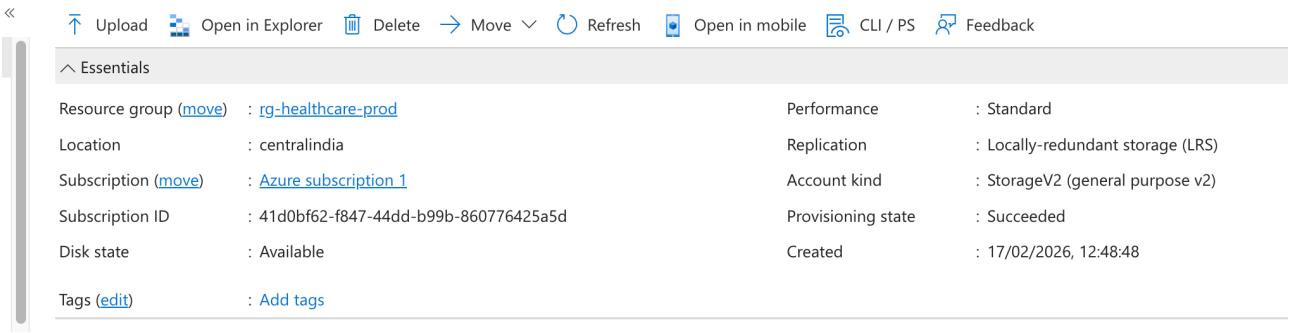
Basics

Subscription	Azure subscription 1
Resource group	rg-healthcare-prod
Location	Central India
Storage account name	sthealthcareprod01
Preferred storage type	
Performance	Standard
Replication	Locally-redundant storage (LRS)

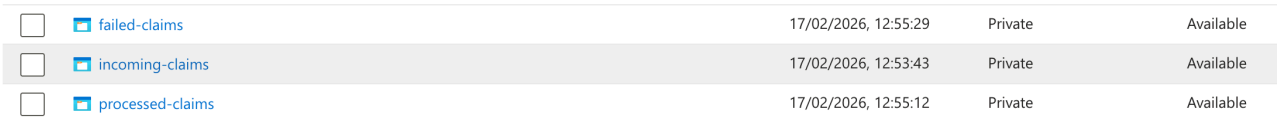
Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot

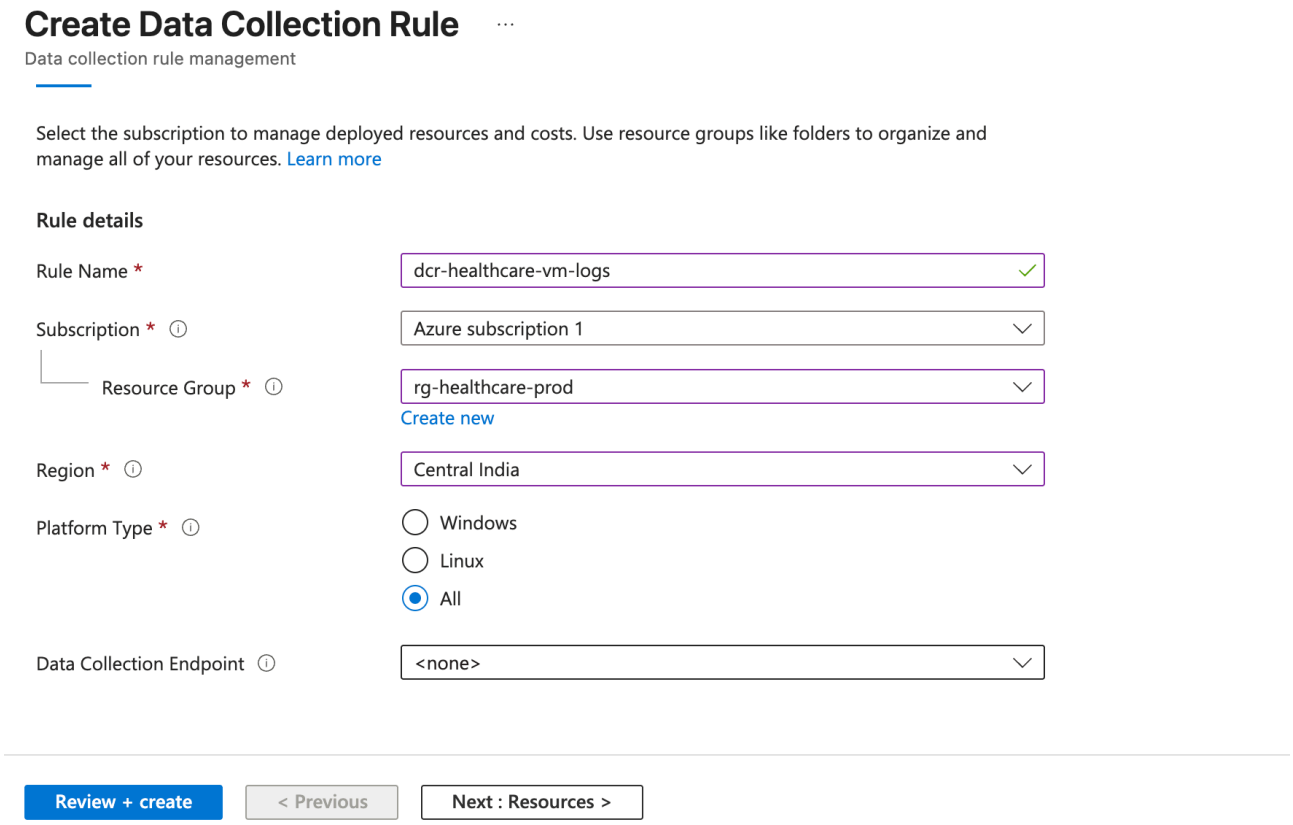
Previous Next Create

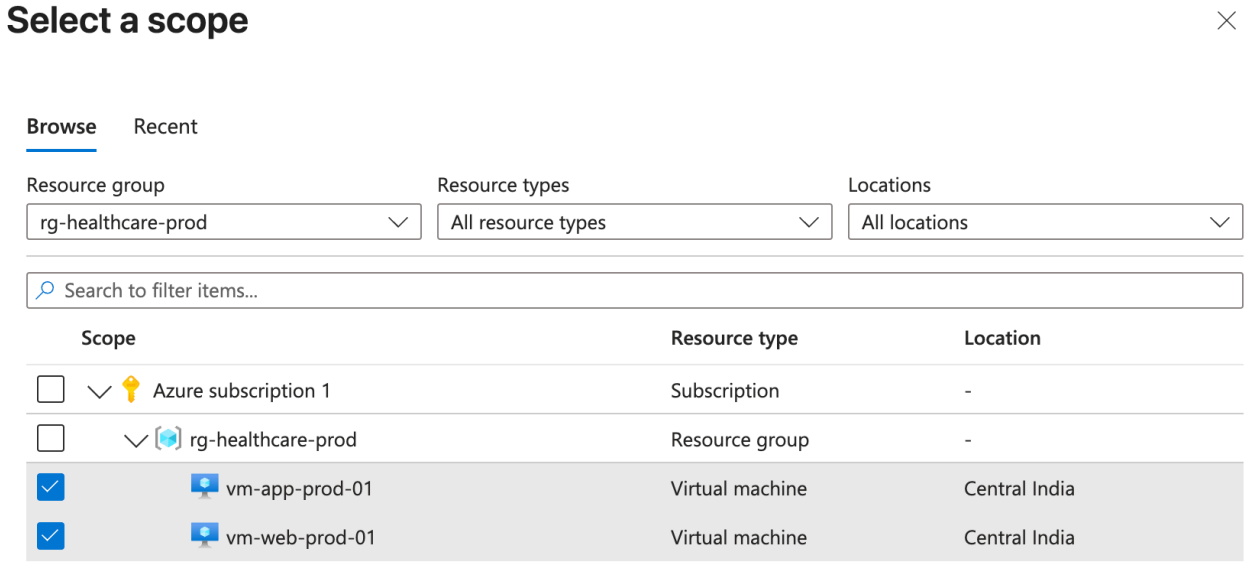


Step-7: Created 3 Blob containers as well, snapshot below:



Step-8: Created Data Collection rule name given dcr-healthcare-vm-logs





Create Data Collection Rule

Data collection rule management

Basics | **Resources** | Collect and deliver | Tags | Review + create

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled servers. For For Windows 10 and 11 devices, download the client installer and follow the guidance

This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

+ Add resources + Create endpoint

Enable Data Collection Endpoints ☑

Only resources in the same region can be assigned to the same endpoint. Learn more

Name	Type	Location	Resource group
vm-app-prod-01	Virtual machine	Central India	rg-healthcare-prod
vm-web-prod-01	Virtual machine	Central India	rg-healthcare-prod

Showing 1 - 2 of 2 results.

Review + create | < Previous | Next : Collect and deliver >

Create Data Collection Rule

Data collection rule management

Validation passed

Basics | Resources | Collect and deliver | Tags | **Review + create**

Basics

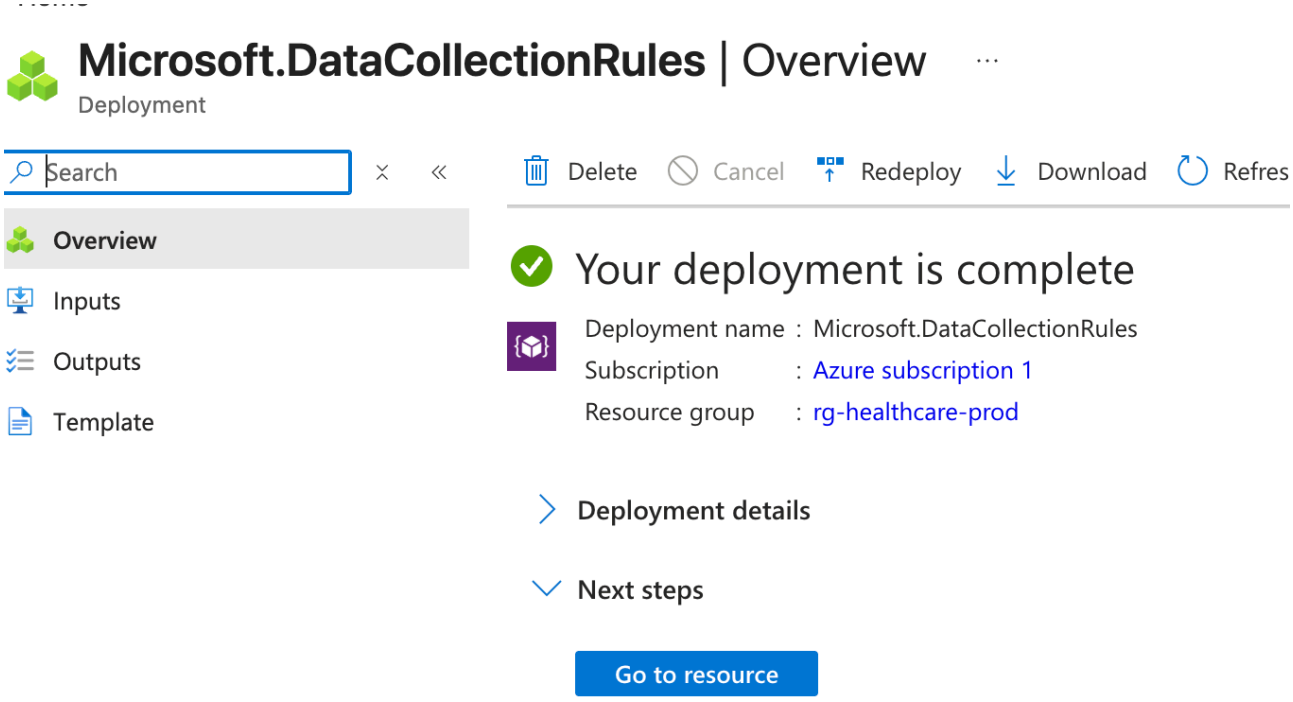
Data rule name	dcr-healthcare-vm-logs
Subscription	Azure subscription 1
Resource Group	rg-healthcare-prod

Selected resources

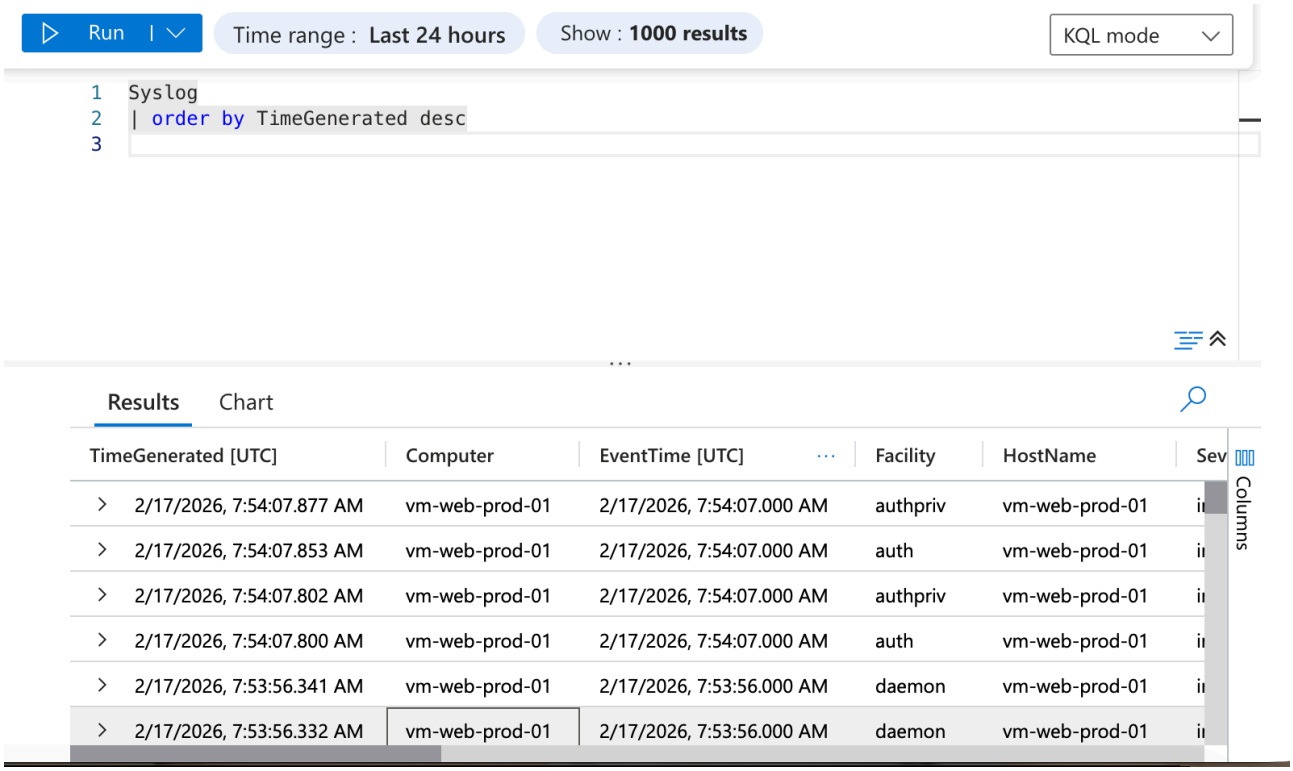
Resources	Type
vm-app-prod-01	microsoft.compute/virtualmachines
vm-web-prod-01	microsoft.compute/virtualmachines

Showing 1 - 2 of 2 results.

Create | < Previous | Next: >



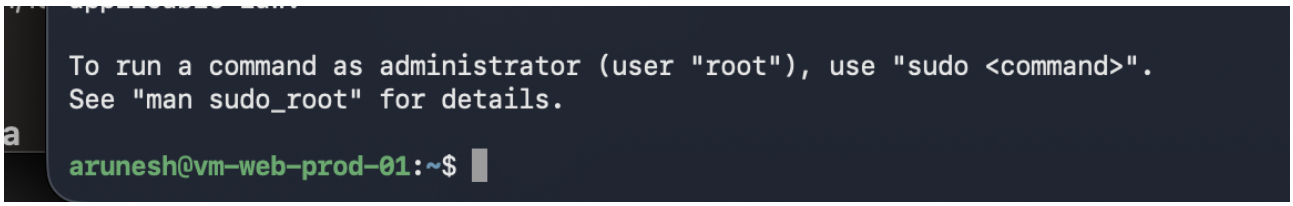
Step-9: Verified logs are coming or not...



Step-10: Then I login to my web vm using the below commands in my local terminal.

ssh -i /Users/aruneshkumartiwari/Downloads/vm-web-prod-01_key.pem arunesh@74.225.252.16

chmod 400 /Users/aruneshkumartiwari/Downloads/vm-web-prod-01_key.pem

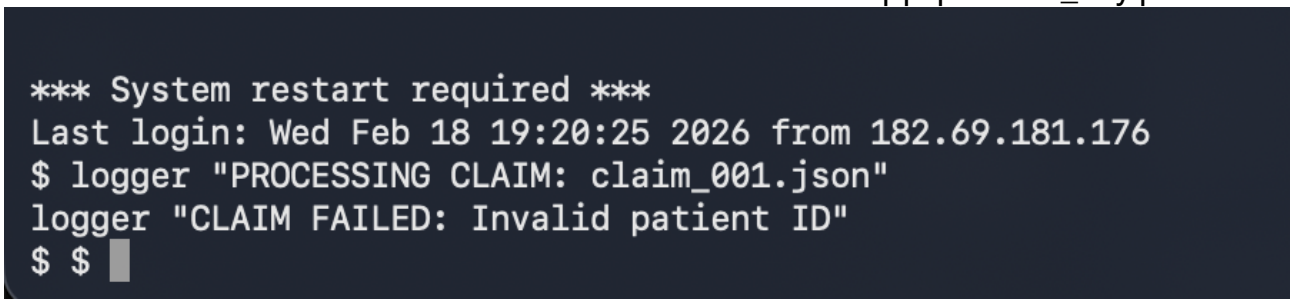


Now I can see my web vm login in my terminal.

Step-11: Now again I tried to app vm in my terminal using the below commands.

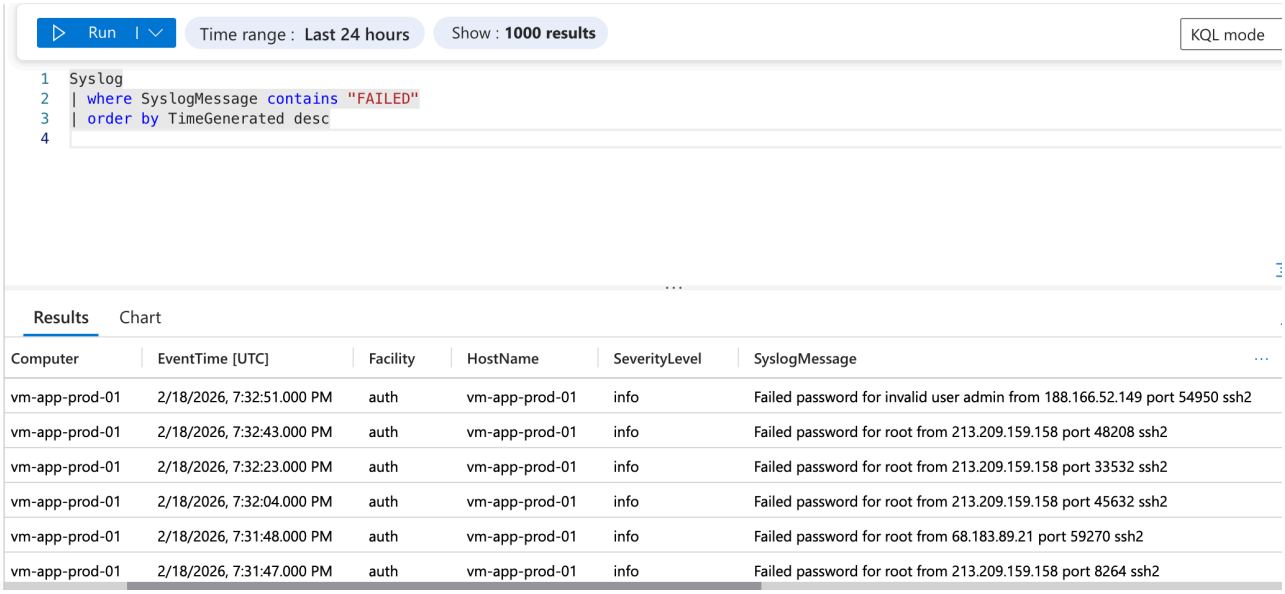
ssh -i /Users/aruneshkumartiwari/Downloads/vm-app-prod-01_key.pem azureuser@20.244.12.129

chmod 400 /Users/aruneshkumartiwari/Downloads/vm-app-prod-01_key.pem



I can see I logged in to my app vm as well.

Step-12: Now I run the below KQL query to check if any records are coming for my vm's.

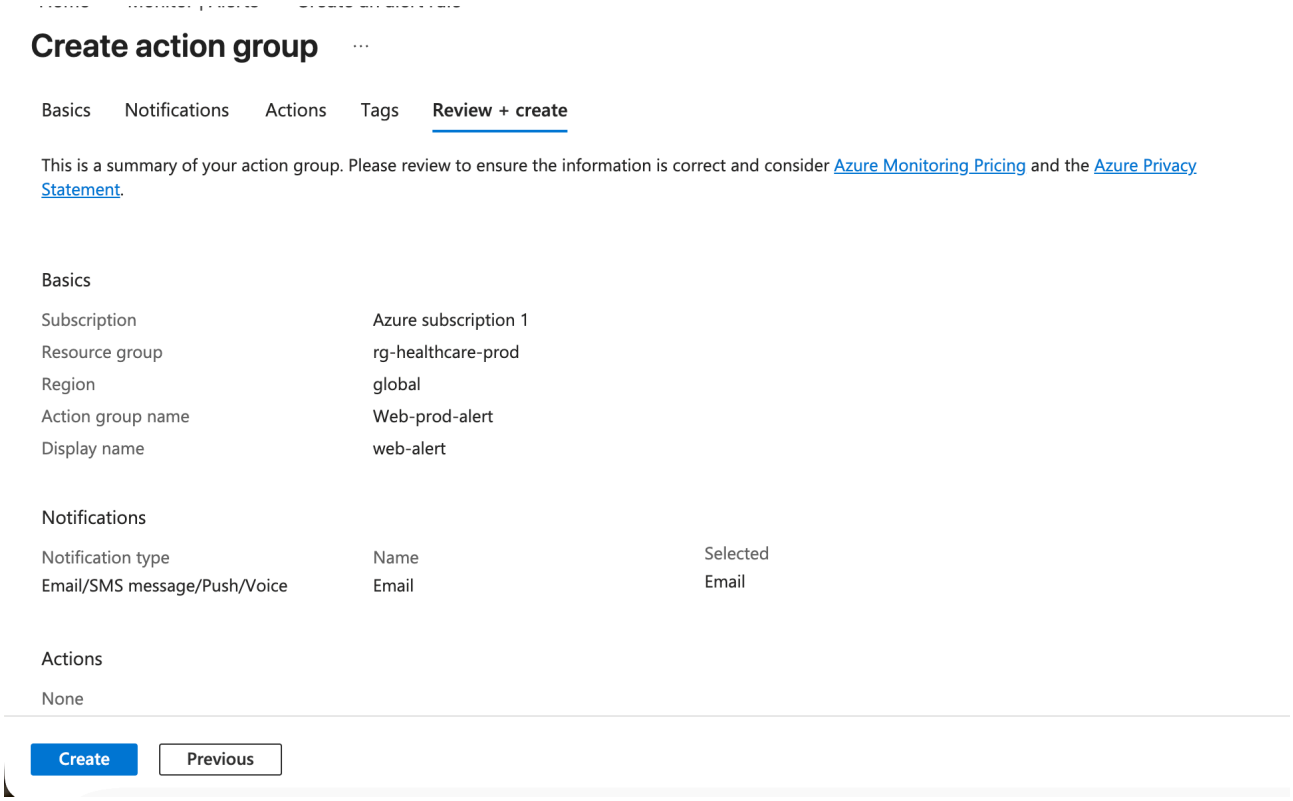


Computer	EventTime [UTC]	Facility	HostName	SeverityLevel	SyslogMessage
vm-app-prod-01	2/18/2026, 7:32:51.000 PM	auth	vm-app-prod-01	info	Failed password for invalid user admin from 188.166.52.149 port 54950 ssh2
vm-app-prod-01	2/18/2026, 7:32:43.000 PM	auth	vm-app-prod-01	info	Failed password for root from 213.209.159.158 port 48208 ssh2
vm-app-prod-01	2/18/2026, 7:32:23.000 PM	auth	vm-app-prod-01	info	Failed password for root from 213.209.159.158 port 33532 ssh2
vm-app-prod-01	2/18/2026, 7:32:04.000 PM	auth	vm-app-prod-01	info	Failed password for root from 213.209.159.158 port 45632 ssh2
vm-app-prod-01	2/18/2026, 7:31:48.000 PM	auth	vm-app-prod-01	info	Failed password for root from 68.183.89.21 port 59270 ssh2
vm-app-prod-01	2/18/2026, 7:31:47.000 PM	auth	vm-app-prod-01	info	Failed password for root from 213.209.159.158 port 8264 ssh2

Step-13: Created a new alert rule.

1. Azure Monitor - Alerts
2. Clicked on Create Alert Rule
3. Scope: Log Analytics Workspace
4. Condition: Custom log search
5. Pasted my KQL query.
6. Threshold: 0
7. Action group: Email
8. Alert name: vm-web-alerts

Name	Condition	Severity	Target scope	Target resource type	Signal type	Status
Vm-web-alerts	Table rows > 0	1 - Error	law-healthcare-prod	Log Analytics workspace	Log search	Enabled



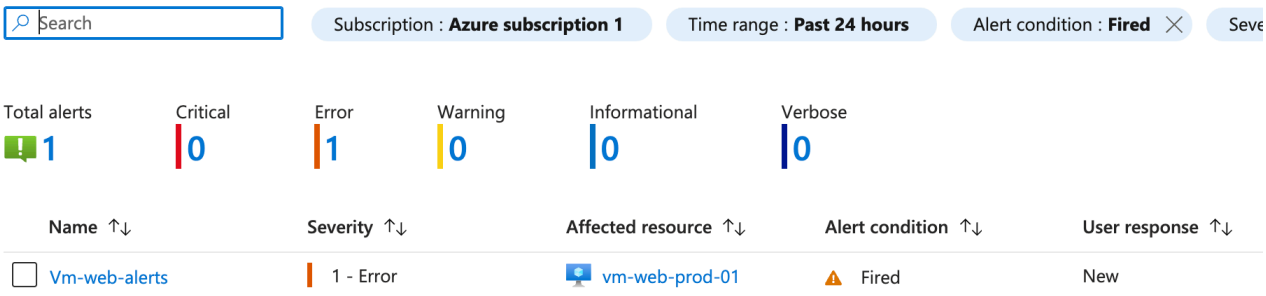
Step-14: Tried to trigger the vm log using the below query under the web vm:

logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"

logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"

```
Try: sudo apt install <deb name>
[arunesh@vm-web-prod-01:~$ logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"
[arunesh@vm-web-prod-01:~$ logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"
[arunesh@vm-web-prod-01:~$ logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"
[arunesh@vm-web-prod-01:~$ logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"
[arunesh@vm-web-prod-01:~$ logger -p local0.err "CLAIM ERROR TEST - HIGH SEVERITY"
```

I got an Alert snapshot for reference.

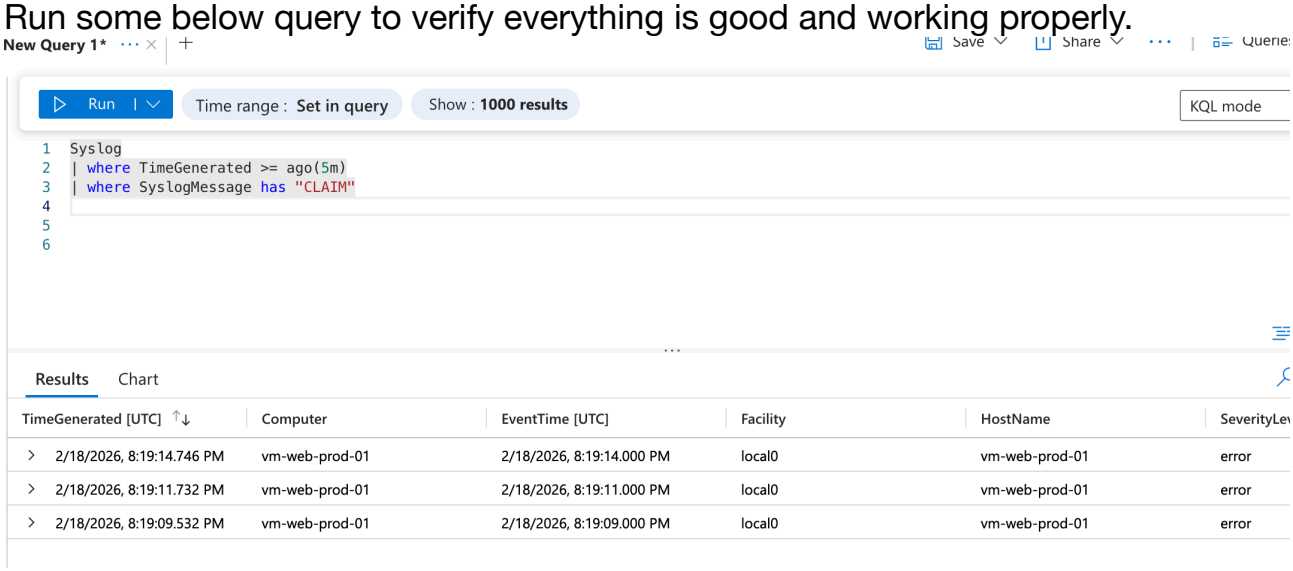


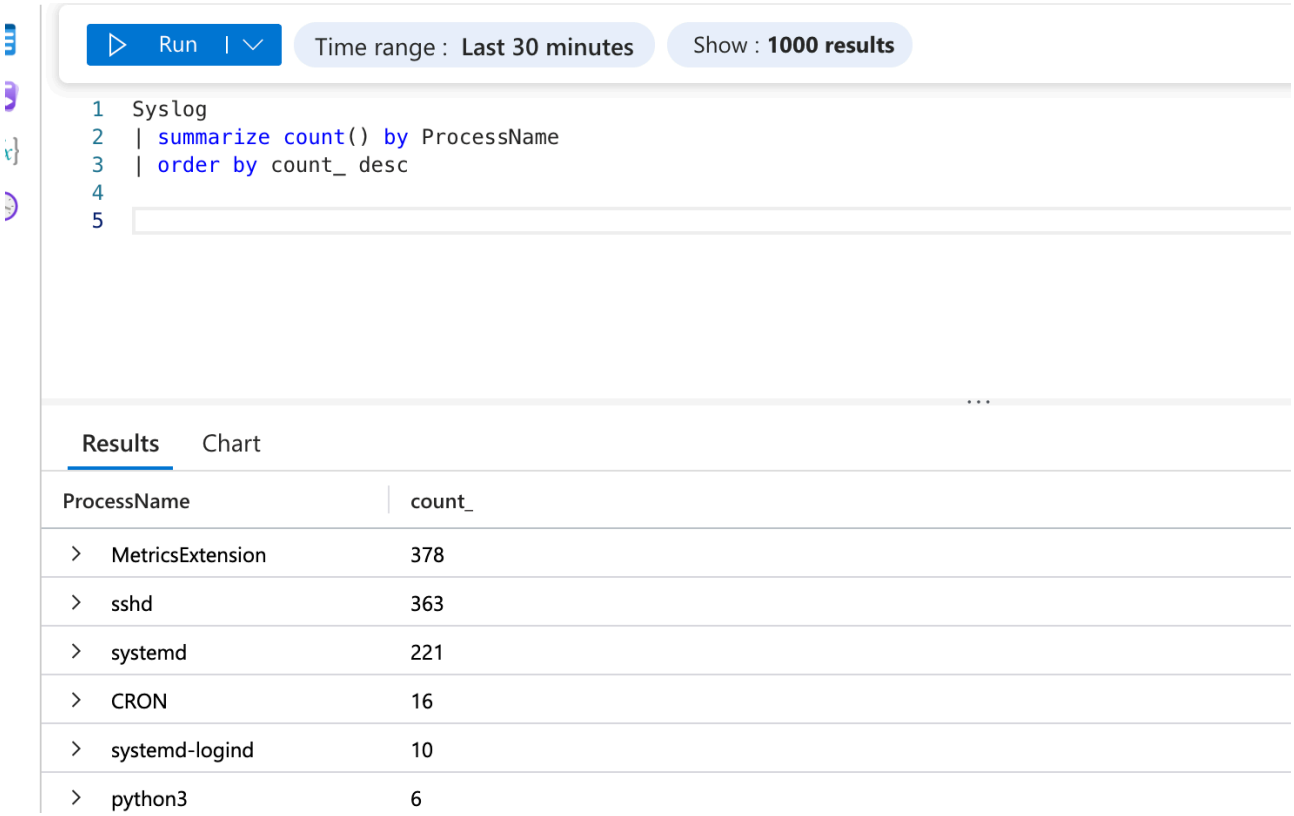
Got an alert on my mail as well.

Summary

Alert name	Vm-web-alerts
Severity	Sev1
Monitor condition	Fired
Affected resource	vm-web-prod-01
Resource type	microsoft.compute/virtualmachines
Resource group	rg-healthcare-prod
Description	There is some spikes in your web vm.
Monitoring service	Log Alerts V2
Signal type	Log
Fired time	February 25, 2026 6:28 UTC

Run some below query to verify everything is good and working properly.





Results & Impact: In this project, I deployed and monitored production VMs using Azure Monitor and Log Analytics. I configured Syslog collection, wrote KQL queries for application log tracking, and implemented real-time alerting for Claim events. I validated alert is triggering or not and email notifications for quicker incident response.