

# Project: Healthcare Claims Processing & Failure Detection Platform

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

```
ResourceGroupName : rg-healthcare-prod
Location         : centralindia
ProvisioningState: Succeeded
Tags             :
ResourceId       : /subscriptions/41d0bf62-f847-44dd-b99b-860776425a5d/resourceGroups/rg-healthcare-prod
PS /home/arunesh> 
```

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

## Create Log Analytics workspace

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

### Project details

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

Subscription \* ⓘ

Subscription dropdown: Azure subscription 1

Resource group \* ⓘ

Resource group dropdown: rg-healthcare-prod

[Create new](#)

### Instance details

Name \* ⓘ

Name input field: law-healthcare-prod

Region \* ⓘ

Region dropdown: Central India

[Review + Create](#)

[« Previous](#)

[Next : Tags >](#)

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
	<a href="#">Create new</a>

### Instance details

Virtual network name *	vnet-healthcare-prod
Region * ⓘ	(Asia Pacific) Central India

[Previous](#)

[Next](#)

[Review + create](#)

Basics Security IP addresses Tags Review + create

10.0.0.0/16	 Delete address space		
10.0.0.0	/16		
10.0.0.0 - 10.0.255.255 65,536 addresses			
Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
AzureFirewallSubnet	10.0.1.0 - 10.0.1.63	/26 (64 addresses)	-

Add IPv4 address space | 

Previous

Next

Review + create

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

### Create a virtual machine



Help me create a VM optimized for high availability

Help me choose the



Help me create a low cost VM

Help me create a VM optimized for high availability

Help me choose the right VM siz

#### 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 machine name \* 

vm-web-prod-01



Region \* 

(Asia Pacific) Central India



[Deploy to an Azure Extended Zone](#)

Availability options 

Availability zone



Zone options 

Self-selected zone

Choose up to 3 availability zones, one VM per zone

Azure-selected zone (Preview)

[< Previous](#)

[Next : Disks >](#)

[Review + create](#)

 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](#)

Virtual network ⓘ

vnet-healthcare-prod (rg-healthcare-prod) ⌄  
Edit virtual network

Subnet \* ⓘ

(New) snet-centralindia-1 ⌄  
Edit subnet 10.0.2.0 - 10.0.2.255 (256 addresses)

Public IP ⓘ

(new) vm-web-prod-01-ip ⌄  
Create new  ⓘ Public IP addresses have a nominal charge. [Estimate price ↗](#)

NIC network security group ⓘ

None  Basic  Advanced

Public inbound ports \* ⓘ

None  Allow selected ports

Select inbound ports \*  ⓘ

HTTP (80), SSH (22) ⌄

[< Previous](#) [Next : Management >](#) [Review + create](#)

## Management Tab - Keep default

Delete Cancel Redeploy Download Refresh

### ... Deployment is in progress

Deployment name: CreateVm-canonical.ubuntu-24\_04-lts-server-2... Start time: 2/17/2026, 12:40:35 PM  
Subscription: [Azure subscription 1](#) Correlation ID: 27f331be-fa56-4509-bd49-179ea95ab6ff

Resource group: rg-healthcare-prod

#### Deployment details

Resource	Type	Status	Operation details
vm-web-prod-01	Microsoft.Compute/virtualMachines	Created	<a href="#">Operation details</a>
vm-web-prod-01613_z1	Microsoft.Network/networkInterfaces	OK	<a href="#">Operation details</a>
network-interface-associated-virt	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
vm-web-prod-01-nsg	Microsoft.Network/networkSecurityGroups	OK	<a href="#">Operation details</a>
vm-web-prod-01-ip	Microsoft.Network/publicIPAddresses	OK	<a href="#">Operation details</a>

Give feedback

Tell us about your experience with deployment

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

<input type="checkbox"/>	Name <span>↑</span>	Subscription	Resource Group	Location	Status	Operating syst...	Size
<input type="checkbox"/>	vm-app-prod-01	...	Azure subscript...	rg-healthcare-p...	Central India	Running	Linux
<input type="checkbox"/>	vm-web-prod-01	...	Azure subscript...	rg-healthcare-p...	Central India	Running	Linux

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

### Create a storage account

Subscription \*

Resource group \*  [Create new](#)

Instance details

Storage account name \*

Region \*  [Deploy to an Azure Extended Zone](#)

Preferred storage type

ⓘ This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance \*  **Standard:** Recommended for most scenarios (general-purpose v2 account)  
 **Premium:** Recommended for scenarios that require low latency.

Redundancy \*

---

[Previous](#) [Next](#) [Review + create](#)

[View automation template](#)

## Basics

Subscription	Azure subscription 1
Resource group	rg-healthcare-prod
Location	Central India
Storage account name	shealthcareprod01
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](#)

« [Upload](#) [Open in Explorer](#) [Delete](#) [Move](#) [Refresh](#) [Open in mobile](#) [CLI / PS](#) [Feedback](#)

^ Essentials

Resource group <a href="#">(move)</a>	: rg-healthcare-prod	Performance	: Standard
Location	: centralindia	Replication	: Locally-redundant storage (LRS)
Subscription <a href="#">(move)</a>	: <a href="#">Azure subscription 1</a>	Account kind	: StorageV2 (general purpose v2)
Subscription ID	: 41d0bf62-f847-44dd-b99b-860776425a5d	Provisioning state	: Succeeded
Disk state	: Available	Created	: 17/02/2026, 12:48:48
Tags <a href="#">(edit)</a>	: <a href="#">Add tags</a>		

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

<input type="checkbox"/>	failed-claims	17/02/2026, 12:55:29	Private	Available
<input type="checkbox"/>	incoming-claims	17/02/2026, 12:53:43	Private	Available
<input type="checkbox"/>	processed-claims	17/02/2026, 12:55:12	Private	Available

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

### Create Data Collection Rule

Data collection rule management

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

#### Rule details

Rule Name \*  ✓

Subscription \*  ▼

Resource Group \*  ▼  
[Create new](#)

Region \*  ▼

Platform Type \*  Windows  
 Linux  
 All

Data Collection Endpoint  ▼

[Review + create](#)

[< Previous](#)

[Next : Resources >](#)

### Select a scope

×

[Browse](#) [Recent](#)

Resource group

▼

Resource types

▼

Locations

▼

Search to filter items...

Scope	Resource type	Location
<input type="checkbox"/> <span>Azure subscription 1</span>	Subscription	-
<input type="checkbox"/> <span>rg-healthcare-prod</span>	Resource group	-
<input checked="" type="checkbox"/> <span>vm-app-prod-01</span>	Virtual machine	Central India
<input checked="" type="checkbox"/> <span>vm-web-prod-01</span>	Virtual machine	Central India

## 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
<a href="#">vm-app-prod-01</a>	microsoft.compute/virtualmachines
<a href="#">vm-web-prod-01</a>	microsoft.compute/virtualmachines

Showing 1 - 2 of 2 results.

[Create](#)

[< Previous](#)

[Next: >](#)

 Microsoft.DataCollectionRules | Overview

Deployment

Search  X << Delete Cancel Redeploy Download Refresh

 Overview

 Inputs

 Outputs

 Template

 Your deployment is complete

Deployment name : Microsoft.DataCollectionRules  
Subscription : Azure subscription 1  
Resource group : rg-healthcare-prod

> Deployment details

▽ Next steps

[Go to resource](#)

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

Run |  Time range : Last 24 hours Show : 1000 results KQL mode

```
1 Syslog
2 | order by TimeGenerated desc
3
```

Results Chart

TimeGenerated [UTC]	Computer	EventTime [UTC]	...	Facility	HostName	Sev
2/17/2026, 7:54:07.877 AM	vm-web-prod-01	2/17/2026, 7:54:07.000 AM		authpriv	vm-web-prod-01	info
2/17/2026, 7:54:07.853 AM	vm-web-prod-01	2/17/2026, 7:54:07.000 AM		auth	vm-web-prod-01	info
2/17/2026, 7:54:07.802 AM	vm-web-prod-01	2/17/2026, 7:54:07.000 AM		authpriv	vm-web-prod-01	info
2/17/2026, 7:54:07.800 AM	vm-web-prod-01	2/17/2026, 7:54:07.000 AM		auth	vm-web-prod-01	info
2/17/2026, 7:53:56.341 AM	vm-web-prod-01	2/17/2026, 7:53:56.000 AM		daemon	vm-web-prod-01	info
2/17/2026, 7:53:56.332 AM	vm-web-prod-01	2/17/2026, 7:53:56.000 AM		daemon	vm-web-prod-01	info

## 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
```

```
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
a arunesh@vm-web-prod-01:~$
```

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
```

```
*** System restart required ***  
Last login: Wed Feb 18 19:20:25 2026 from 182.69.181.176  
$ logger "PROCESSING CLAIM: claim_001.json"  
logger "CLAIM FAILED: Invalid patient ID"  
$ $
```

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.**

Run | ⏪
Time range : Last 24 hours
Show : 1000 results
KQL mode

```

1 Syslog
2 | where SyslogMessage contains "FAILED"
3 | order by TimeGenerated desc
4

```

Results    Chart

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 ↑↓
<input type="checkbox"/> <a href="#">Vm-web-alerts</a>	Table rows > 0	1 - Error	law-healthcare-prod	Log Analytics workspace	Log search	<span>Enabled</span>

## Create action group

Basics Notifications Actions Tags **Review + create**

This is a summary of your action group. Please review to ensure the information is correct and consider [Azure Monitoring Pricing](#) and the [Azure Privacy Statement](#).

### Basics

Subscription Azure subscription 1  
Resource group rg-healthcare-prod  
Region global  
Action group name Web-prod-alert  
Display name web-alert

### Notifications

Notification type Name Selected  
Email/SMS message/Push/Voice Email

### Actions

None

**Create**

[Previous](#)

## 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.

The screenshot shows the Azure Alert Snapshot interface. At the top, there are filters for 'Search', 'Subscription: Azure subscription 1', 'Time range: Past 24 hours', 'Alert condition: Fired', and 'Severity'. Below these, a summary table shows the count of alerts for different severities: Total alerts (1), Critical (1), Error (1), Warning (0), Informational (0), and Verbose (0). A table then lists the single alert: 'Vm-web-alerts' (Severity 1 - Error) on 'vm-web-prod-01' with the status 'Fired' and 'New'.

Name	Severity	Affected resource	Alert condition	User response
Vm-web-alerts	1 - Error	vm-web-prod-01	Fired	New

Got an alert on my mail as well.

INVESTIGATE  

VIEW THE ALERT IN AZURE MONITOR  

## Summary

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

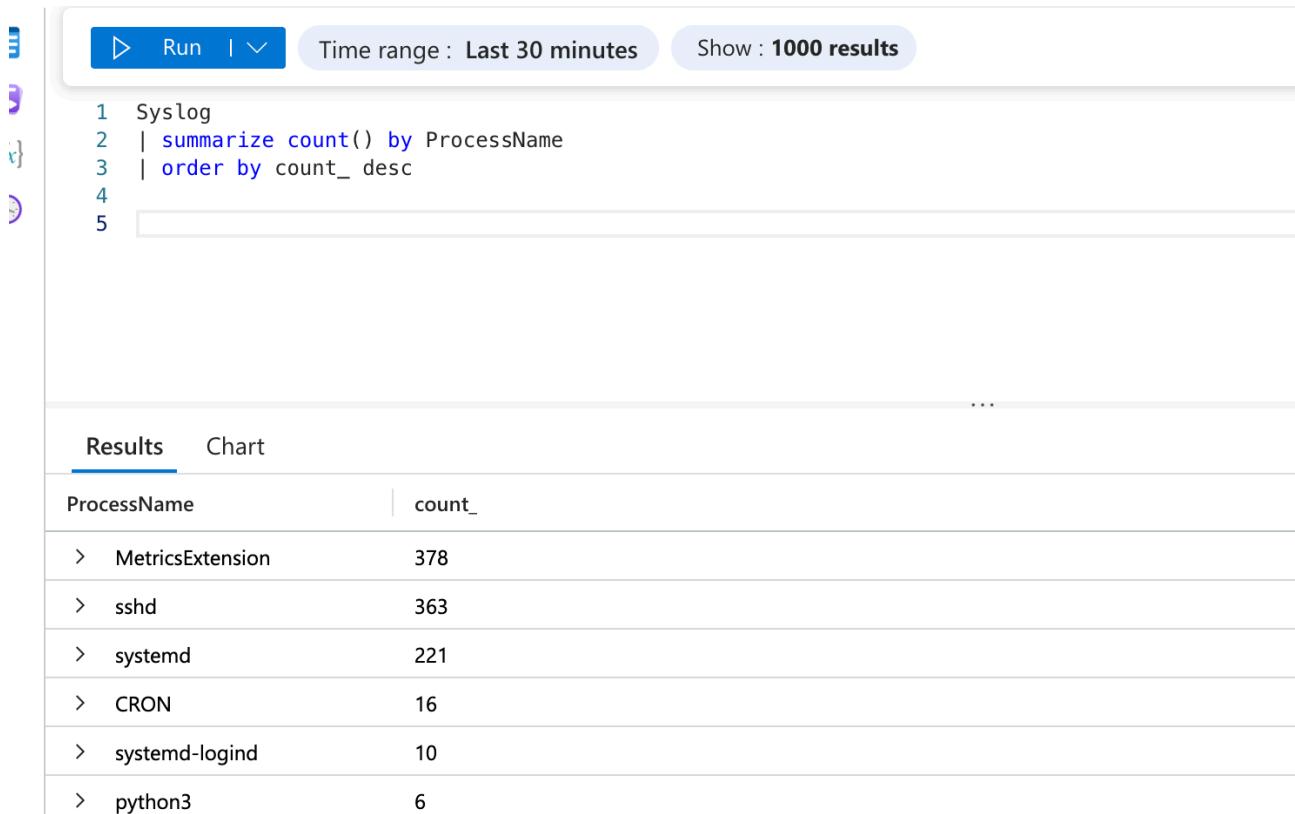
Run some below query to verify everything is good and working properly.

New Query 1\* ... + + Time range : Set in query Show : 1000 results Save Share ... Queue KQL mode

```
1 Syslog
2 | where TimeGenerated >= ago(5m)
3 | where SyslogMessage has "CLAIM"
4
5
6
```

Results Chart

TimeGenerated [UTC] <span style="border: 1px solid black; padding: 2px 5px;">↑</span>	Computer	EventTime [UTC]	Facility	HostName	SeverityLevel
> 2/18/2026, 8:19:14.746 PM	vm-web-prod-01	2/18/2026, 8:19:14.000 PM	local0	vm-web-prod-01	error
> 2/18/2026, 8:19:11.732 PM	vm-web-prod-01	2/18/2026, 8:19:11.000 PM	local0	vm-web-prod-01	error
> 2/18/2026, 8:19:09.532 PM	vm-web-prod-01	2/18/2026, 8:19:09.000 PM	local0	vm-web-prod-01	error



The screenshot shows the Azure Log Analytics workspace interface. At the top, there are navigation icons (File, Run, Save, etc.), a time range selector set to 'Last 30 minutes', and a results count indicator 'Show : 1000 results'. Below this is a code editor window containing a KQL query:

```
1 Syslog
2 | summarize count() by ProcessName
3 | order by count_ desc
4
5
```

Below the code editor is a results table with two columns: 'ProcessName' and 'count\_'. The table lists the following data:

ProcessName	count_
> MetricsExtension	378
> sshd	363
> systemd	221
> CRON	16
> systemd-logind	10
> python3	6

**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.