Centralized Logging & Incident Analysis Platform

STEP 1: I Create a Resource Group:

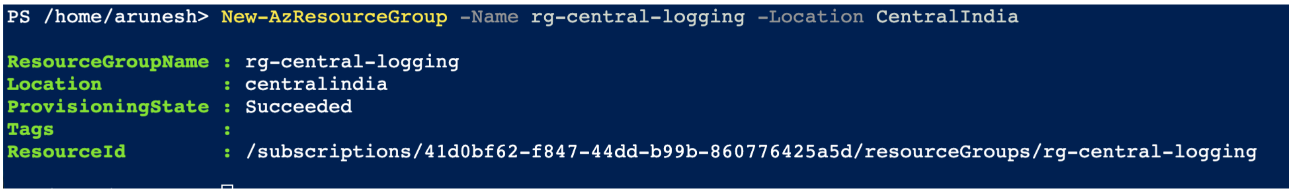
1. I Go to Azure Portal
2. Search **Resource Groups**
3. Click on **Create**

Fill:

- Resource Group Name: rg-central-logging-sre
- Region: Central India (any region is OK)

Click **Review + Create**

I used below script to create a Resource Group.



```
PS /home/arunesh> New-AzResourceGroup -Name rg-central-logging -Location CentralIndia

ResourceGroupName : rg-central-logging
Location          : centralindia
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/41d0bf62-f847-44dd-b99b-860776425a5d/resourceGroups/rg-central-logging
```

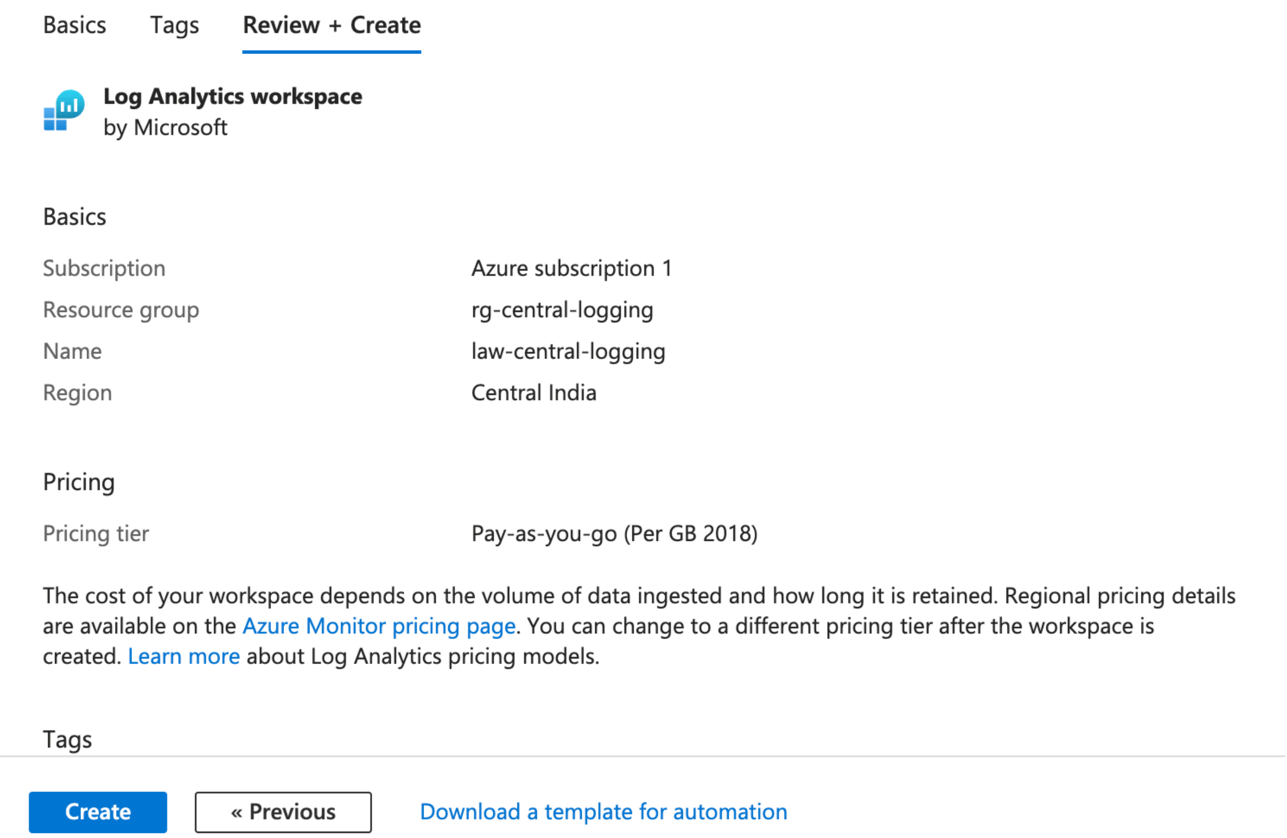
STEP 2: I Created Log Analytics Workspace using the below steps:

1. I Search Log Analytics Workspaces
2. Clicked on Create

Fill:

- Name given: law-central-logging-sre
- Resource Group given: rg-central-logging-sre
- Region: Same as VM (recommended)

Click **Review + Create**



Log Analytics workspace
by Microsoft

Basics

Subscription	Azure subscription 1
Resource group	rg-central-logging
Name	law-central-logging
Region	Central India

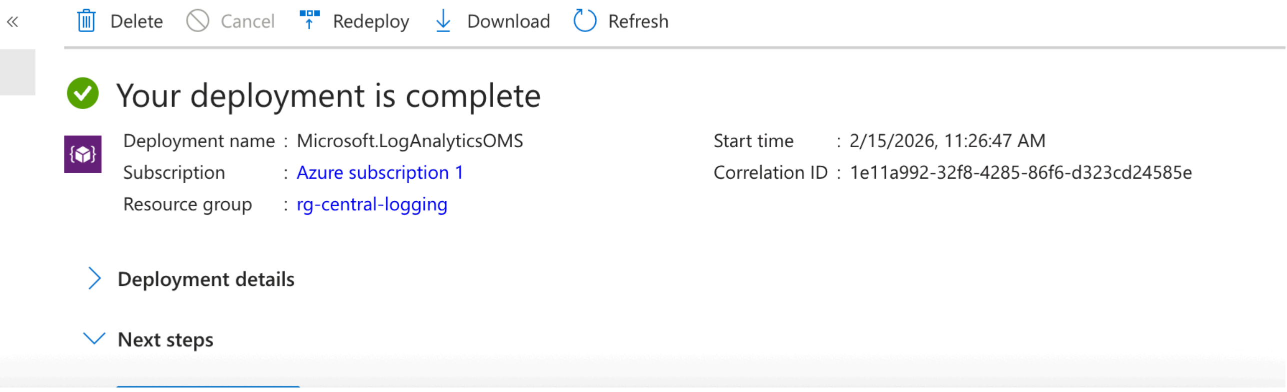
Pricing

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. Regional pricing details are available on the Azure Monitor pricing page. You can change to a different pricing tier after the workspace is created. Learn more about Log Analytics pricing models.

Tags

Once I click Create then it created log analytics workspace.



Your deployment is complete

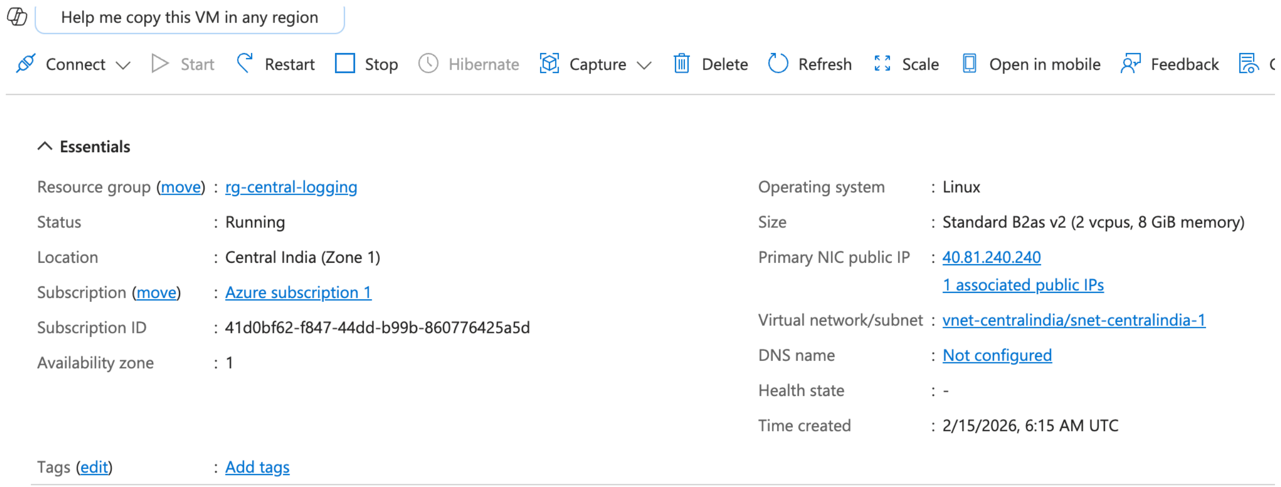
Deployment name : Microsoft.LogAnalyticsOMS
Subscription : Azure subscription 1
Resource group : rg-central-logging

Start time : 2/15/2026, 11:26:47 AM
Correlation ID : 1e11a992-32f8-4285-86f6-d323cd24585e

STEP 3: I Created a Linux VM

Search Virtual Machine
Clicked on Create button
Used the existing Resource Group

- Image given: Ubuntu LTS
- Size provided: Free tier eligible
- Authentication: SSH



Essentials

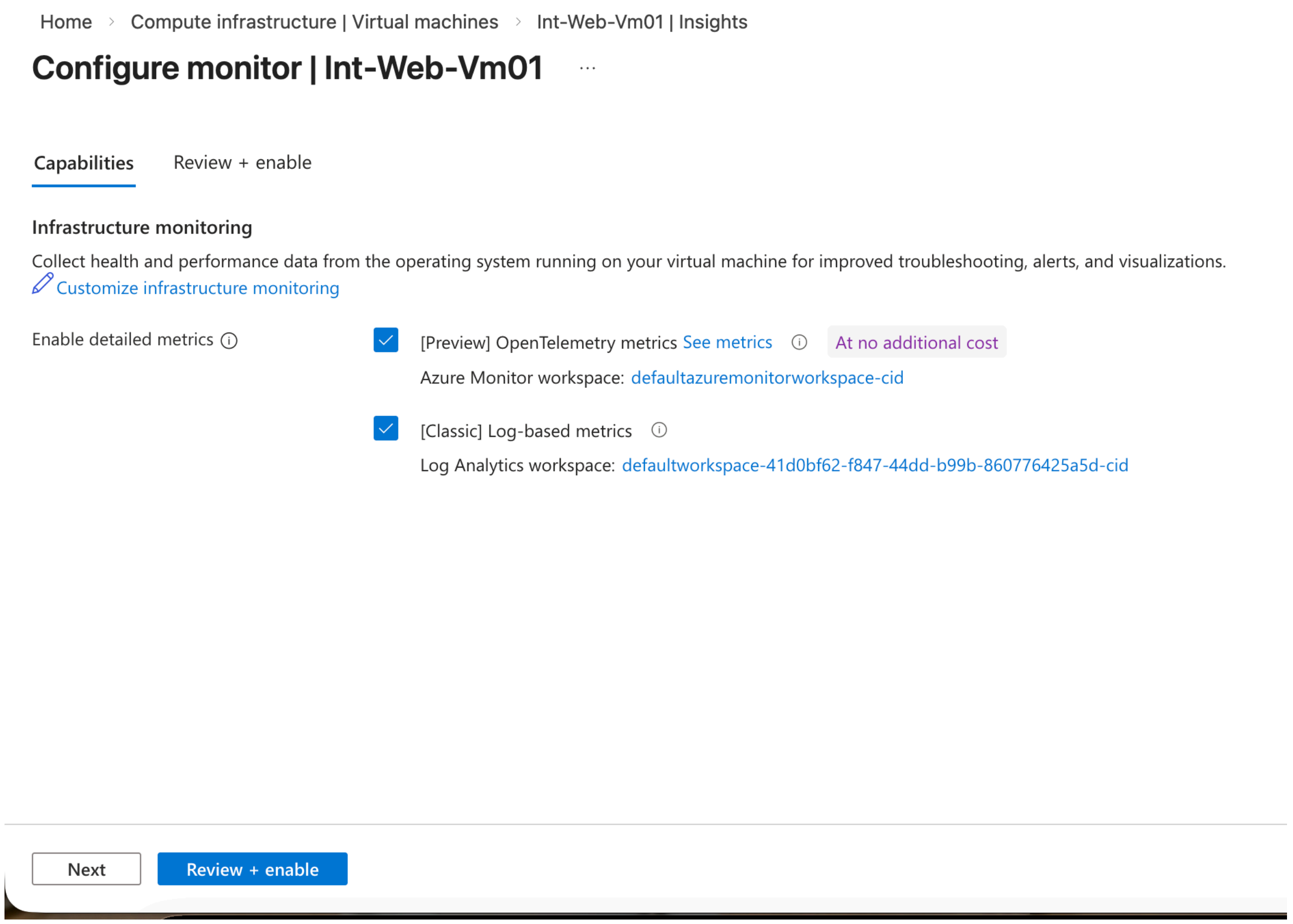
Resource group (move)	: rg-central-logging	Operating system	: Linux
Status	: Running	Size	: Standard B2as v2 (2 vcpus, 8 GiB memory)
Location	: Central India (Zone 1)	Primary NIC public IP	: 40.81.240.240 1 associated public IPs
Subscription (move)	: Azure subscription 1	Virtual network/subnet	: vnet-centralindia/snet-centralindia-1
Subscription ID	: 41d0bf62-f847-44dd-b99b-860776425a5d	DNS name	: Not configured
Availability zone	: 1	Health state	: -
		Time created	: 2/15/2026, 6:15 AM UTC
Tags (edit)	: Add tags		

STEP 4: Connected VM to Log Analytics Workspace

Because without this, logs will not flow.

Steps performed:

1. Opened Virtual Machine
2. Go to Monitoring then click on Insights
3. Clicked on Enable


Home › Compute infrastructure | Virtual machines › Int-Web-Vm01 | Insights
Capabilities
Review + enable
Next
Review + enable

Configure monitor | Int-Web-Vm01

Infrastructure monitoring

Collect health and performance data from the operating system running on your virtual machine for improved troubleshooting, alerts, and visualizations.

Customize infrastructure monitoring

Enable detailed metrics

☑ [Preview] OpenTelemetry metrics See metrics — At no additional cost

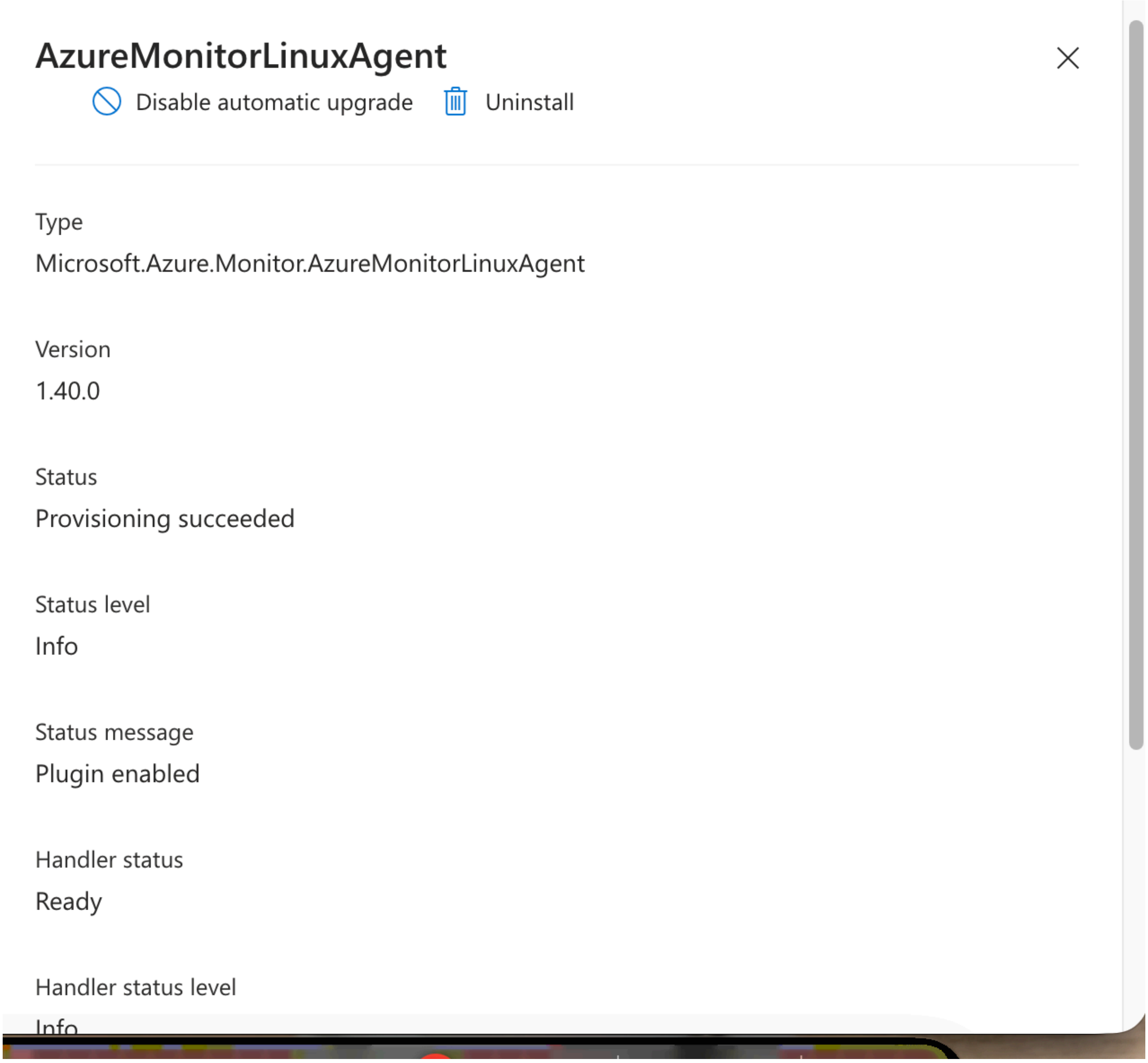
Azure Monitor workspace: defaultazuremonitorworkspace-cid

☑ [Classic] Log-based metrics

Log Analytics workspace: defaultworkspace-41d0bf62-f847-44dd-b99b-860776425a5d-cid

STEP 5 A: Azure Monitor Agent Is Installed
Steps:

1. Opened **Virtual Machine**
2. Go to **Extensions + Applications**
1. Click **Add**
2. Select **Azure Monitor Agent**
3. Click **Create**



AzureMonitorLinuxAgent

Type
Microsoft.Azure.Monitor.AzureMonitorLinuxAgent

Version
1.40.0

Status
Provisioning succeeded

Status level
Info

Status message
Plugin enabled

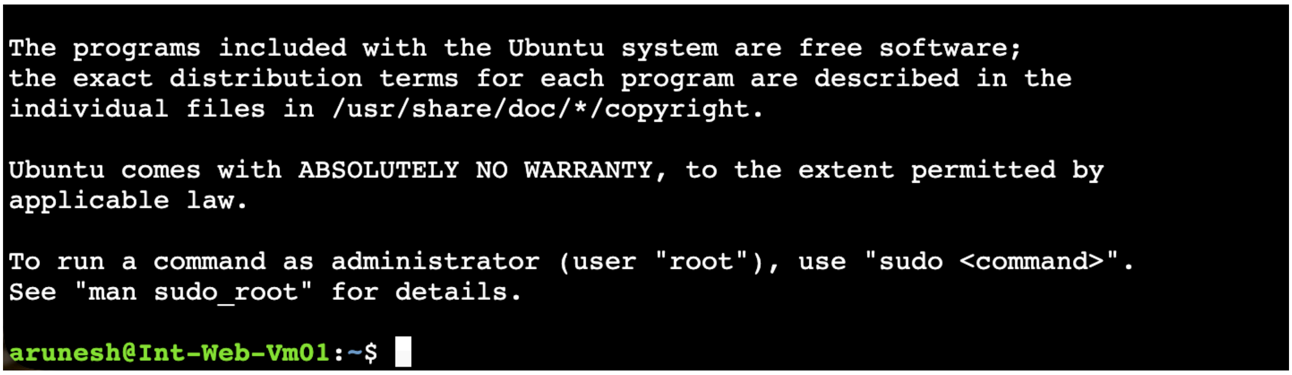
Handler status
Ready

Handler status level
Info

STEP 6: Generated Logs (Real Incident Simulation)
SSH into VM

```
ssh azureuser@<VM-PUBLIC-IP>
```

When you see something like this then you need to perform below commands.



```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

arunesh@Int-Web-Vm01:~$
```

Generated logs using the below queries:

sudo apt update
sudo apt install apache2 -y
sudo systemctl restart apache2
sudo systemctl stop apache2
This basically creates:

- System logs
- Service failure logs

Created Data Collection Rule > Resources
What to do on this screen

1. Selected **Int-Web-Vm01**
2. Clicked on **Apply**
3. Clicked on **Next: Collect and deliver**

This step only links the VM to the DCR.

Next Screen: "Collect and deliver"
Clicked on Add data source
You will see options like:

- Performance counters
- Logs
- Syslog (Linux)

Select Logs
Chooses:

- **Linux syslog**

Why I used this:

- Heartbeat is sent automatically
- Syslog enables real incident analysis

Click on **Next**

Configure Syslog (MANDATORY)
Select:

- Facilities: **auth, daemon, syslog**
- Log levels: **Info, Warning, Error, Critical**

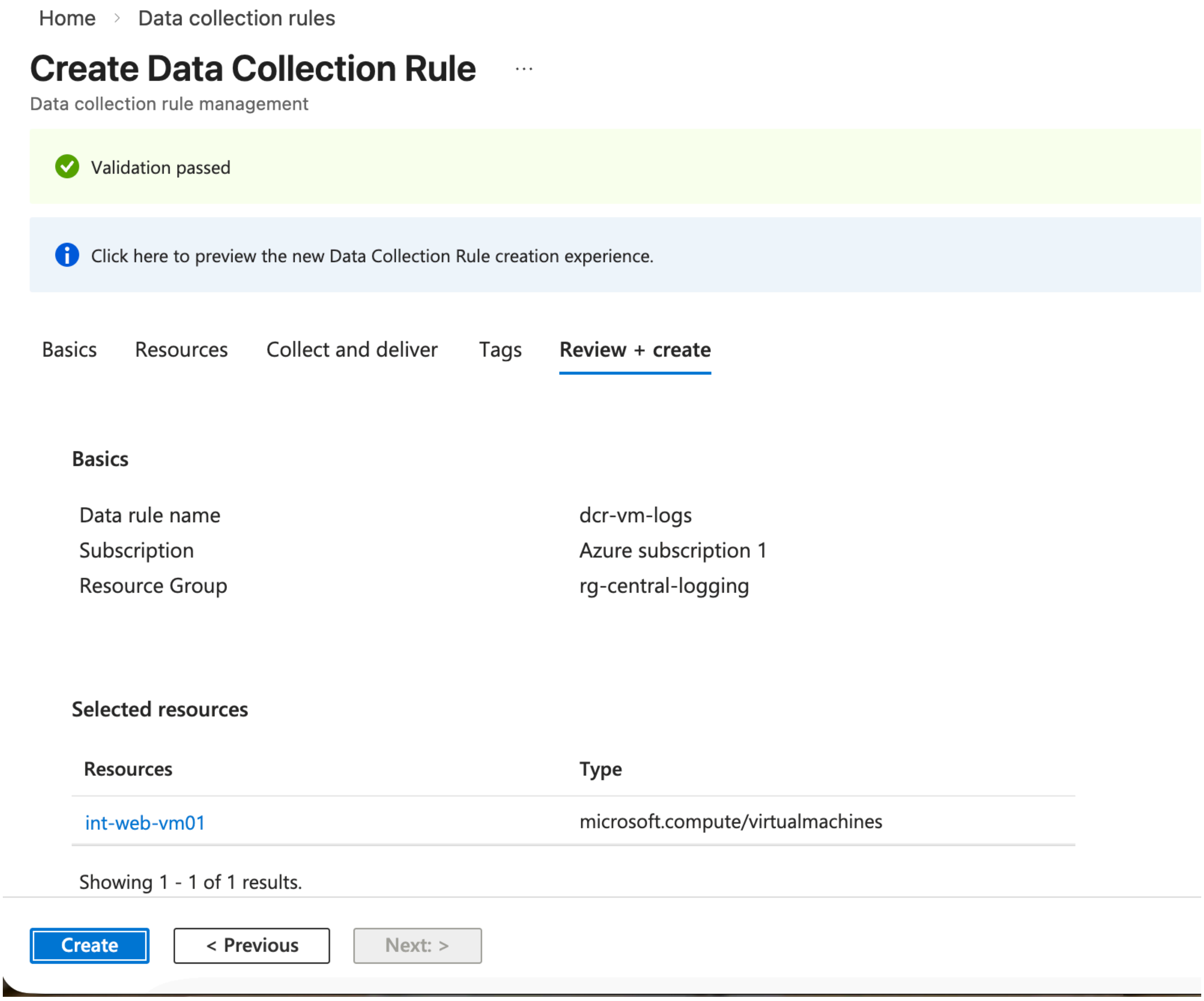
This ensures logs actually flow.

Destination
Selected:

- **Log Analytics workspace**

- Chooses my existing workspace

Click Add > Next > Create



Home › Data collection rules

Create Data Collection Rule ...

Data collection rule management

Validation passed

Click here to preview the new Data Collection Rule creation experience.

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

Basics

Data rule name	dcr-vm-logs
Subscription	Azure subscription 1
Resource Group	rg-central-logging

Selected resources

Resources	Type
int-web-vm01	microsoft.compute/virtualmachines

Showing 1 - 1 of 1 results.

WAIT TIME

After creating DCR:

- Waited for 5–10 minutes
- Because Azure Monitor is not instant

Verified the heartbeat (run the query below)

I go to:

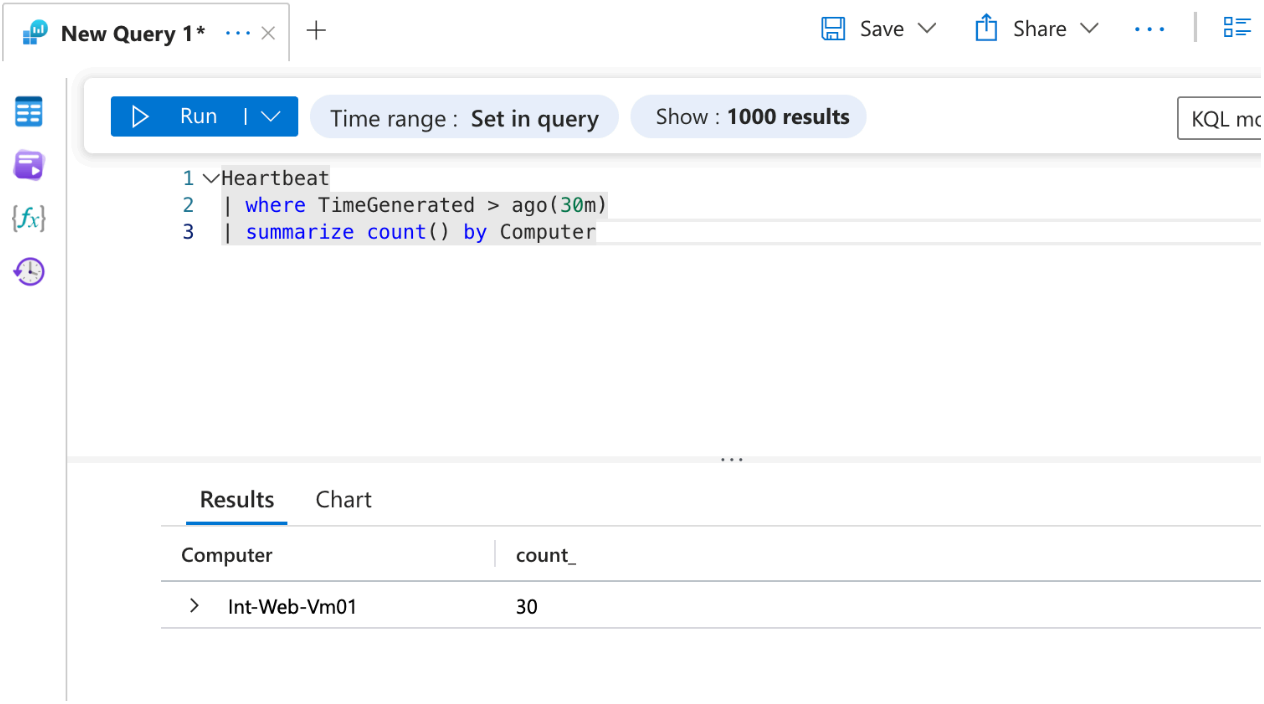
Log Analytics > Logs

Run the below query:

```
Heartbeat
| where TimeGenerated > ago(30m)
| summarize count() by Computer
```

You SHOULD see:

- Int-Web-Vm01
- Count value > 0

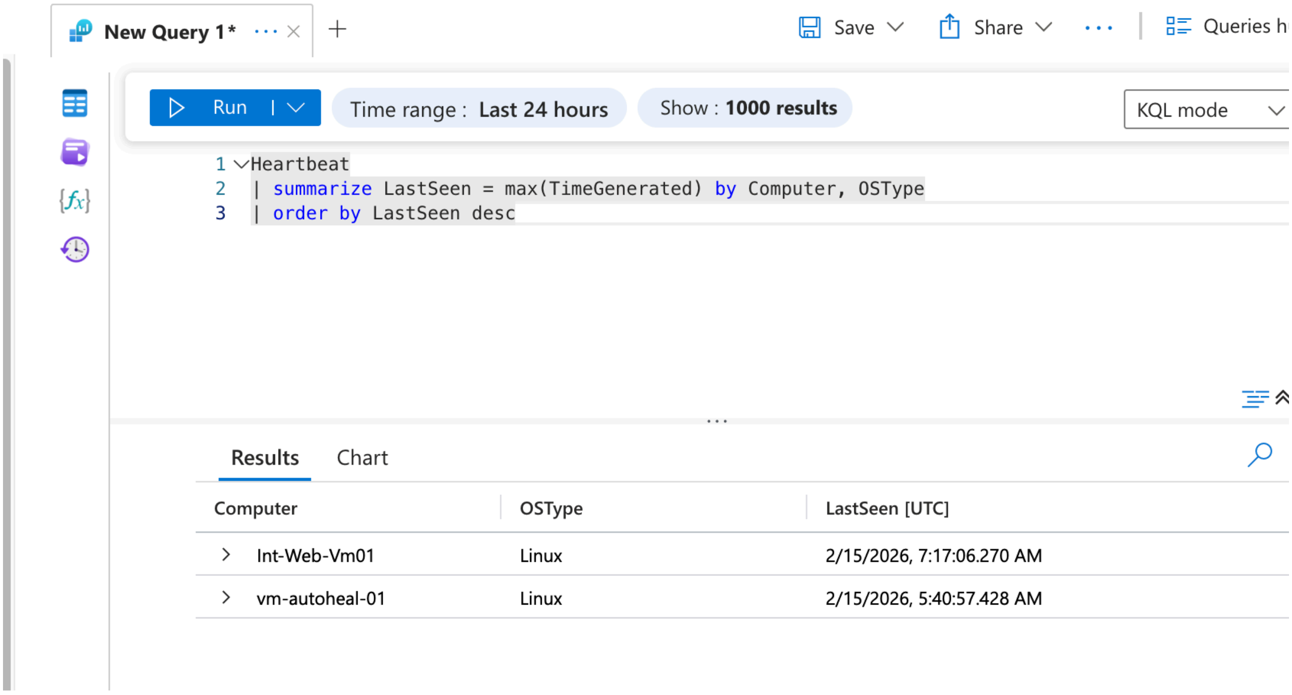


```
Heartbeat
| where TimeGenerated > ago(30m)
| summarize count() by Computer
```

Computer	count_
Int-Web-Vm01	30

More KQL query ran to verify:

Heartbeat
| summarize LastSeen = max(TimeGenerated) by Computer, OSType
| order by LastSeen desc

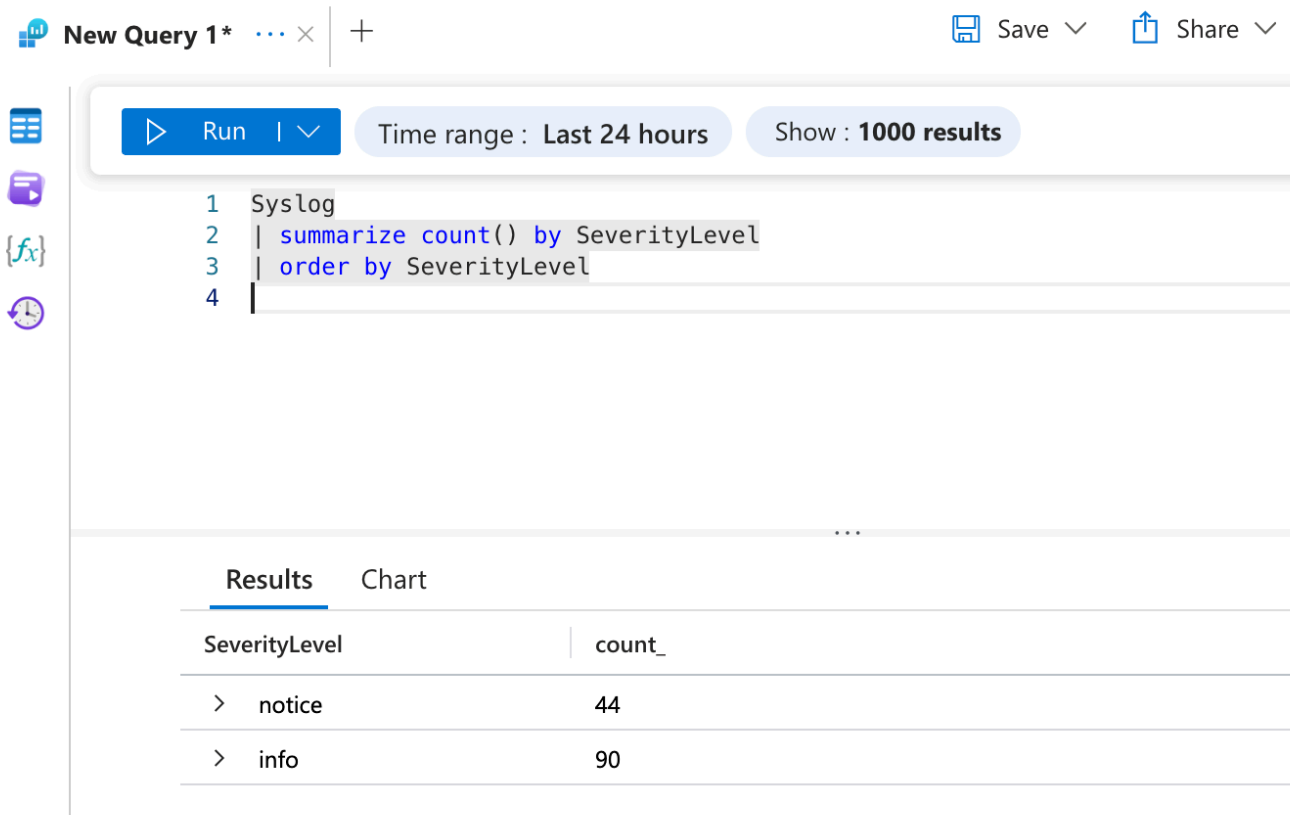


```
Heartbeat
| summarize LastSeen = max(TimeGenerated) by Computer, OSType
| order by LastSeen desc
```

Computer	OSType	LastSeen [UTC]
Int-Web-Vm01	Linux	2/15/2026, 7:17:06.270 AM
vm-autoheal-01	Linux	2/15/2026, 5:40:57.428 AM

Confirmed agent is installed and connected
Shows Linux my OSType that I created
Shows last contact time

Syslog
| summarize count() by SeverityLevel
| order by SeverityLevel



```
Syslog
| summarize count() by SeverityLevel
| order by SeverityLevel
```

SeverityLevel	count_
notice	44
info	90

Project Outcome & Learnings:

I checked what severities are actually coming.

I created a Log Analytics Workspace to store all system and application logs.

I connected my virtual machine to Azure Monitor using a Data Collection Rule.

I enabled Syslog and Heartbeat data so the VM can send health and system logs.

I verified agent connectivity by checking the Heartbeat table in Log Analytics.

I used KQL queries to filter Syslog data for daemon and system-level errors.

Finally, I confirmed logs were flowing correctly by sorting data using TimeGenerated.