Project : Auto-Healing Infrastructure

STEP 1: Create Resource Group

1. Azure Portal > **Resource Groups**
2. Click **Create**
3. Name: rg-auto-healing-sre
4. Region: Central India (or nearest)
5. Click **Create**

Or

Go to Azure Cloud-Shell > Powershell
Write a script:
New-AzResourceGroup -Name YourResourceGroupName -Location YourLocation
Snapshot for reference:

```
PS /home/arunesh> New-AzResourceGroup -Name rg-auto-healing-sre -Location CentralIndia

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

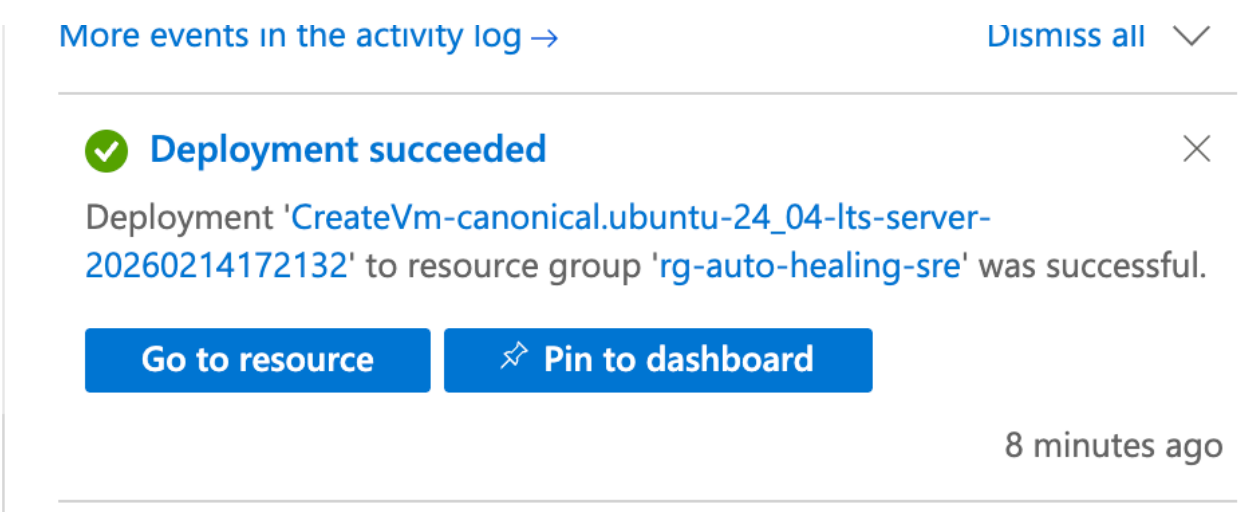
STEP 2: Create Virtual Machine (Problem Target)

1. Azure Portal **> Virtual Machines**
2. Click **Create > Azure Virtual Machine**
3. Settings:

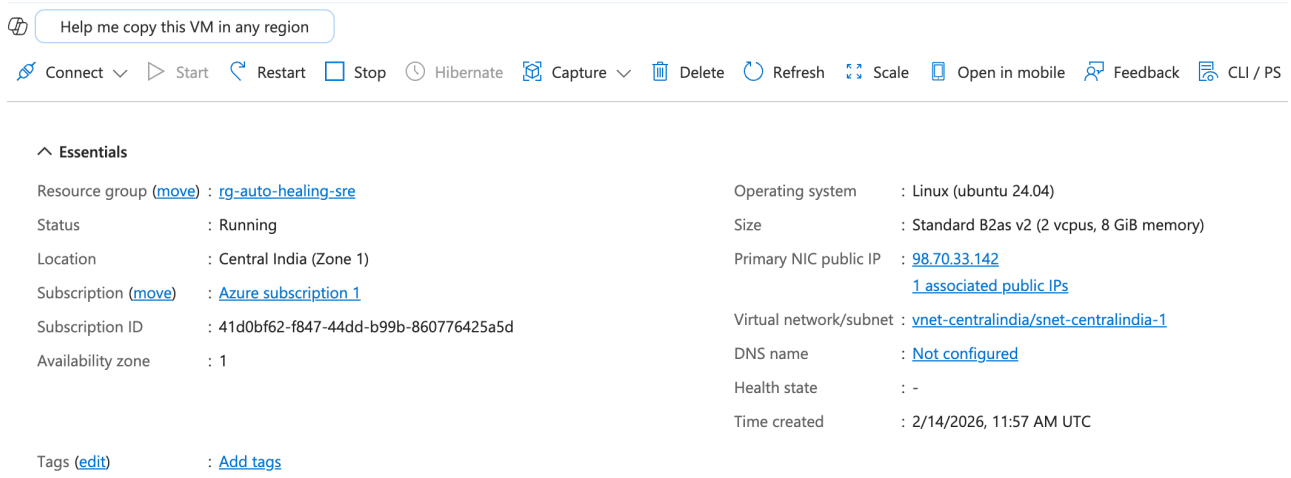
- Name: vm-autoheal-01
- Image: Ubuntu 24.04 LTS
- Size: Standard B2as v2
- Authentication: Password or SSH

4. Networking > keep defaults
5. Click **Create.**

Once Vm deployed you will see messages below like this:

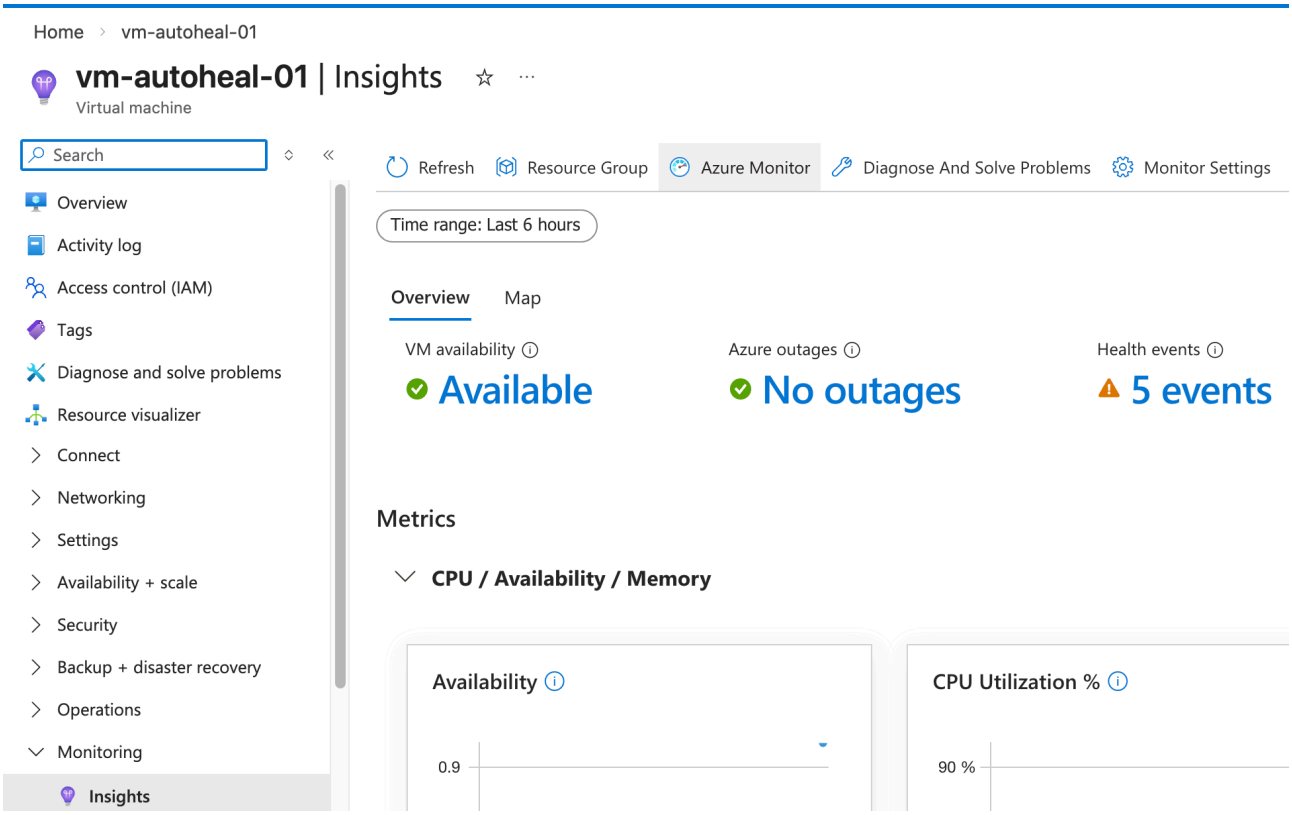


Below Snapshot for the reference:



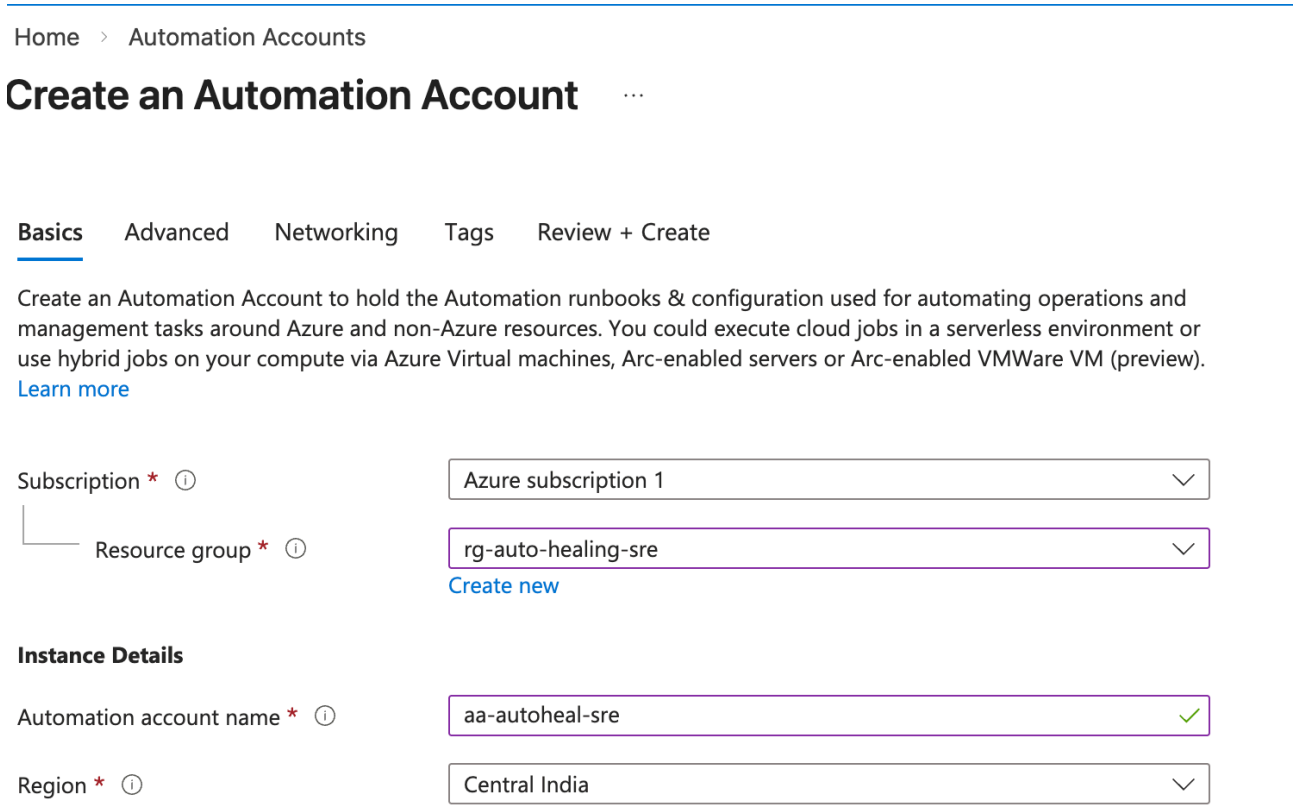
STEP 3: Enable Monitoring

1. Open VM > **Monitoring > Insights > Monitor Settings**
2. Click **Enable**
3. Create **Log Analytics Workspace**
   - Name: vm-autoheal-01
4. Enable



STEP 4: Create Automation Account (Auto-Fix Engine)

1. Azure Portal > **Automation Accounts**
2. Click **Create**
3. Name: aa-autoheal-sre
4. Enable **System Assigned Managed Identity**
5. Create



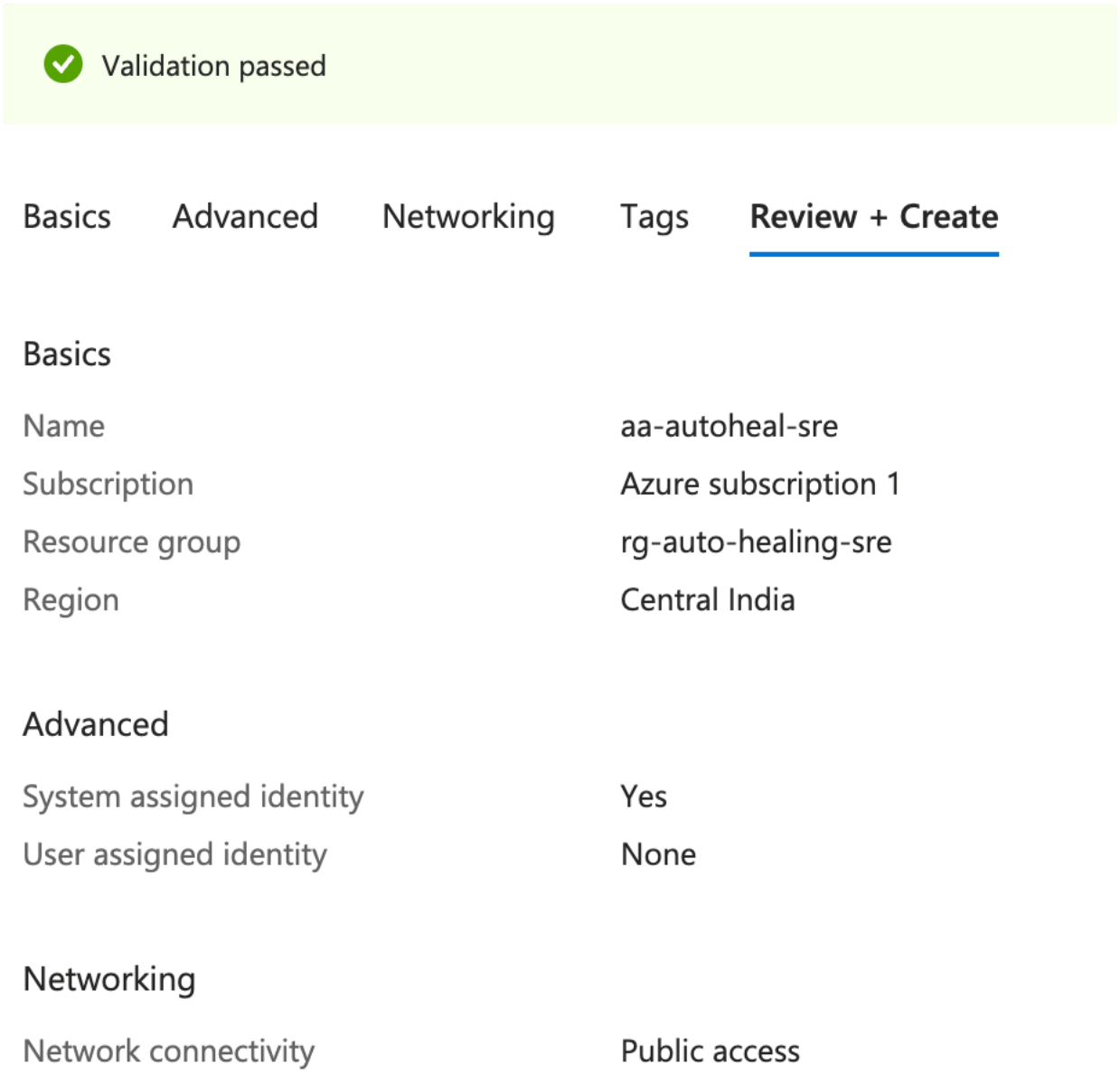
Basics **Advanced** Networking Tags Review + Create

Managed Identities

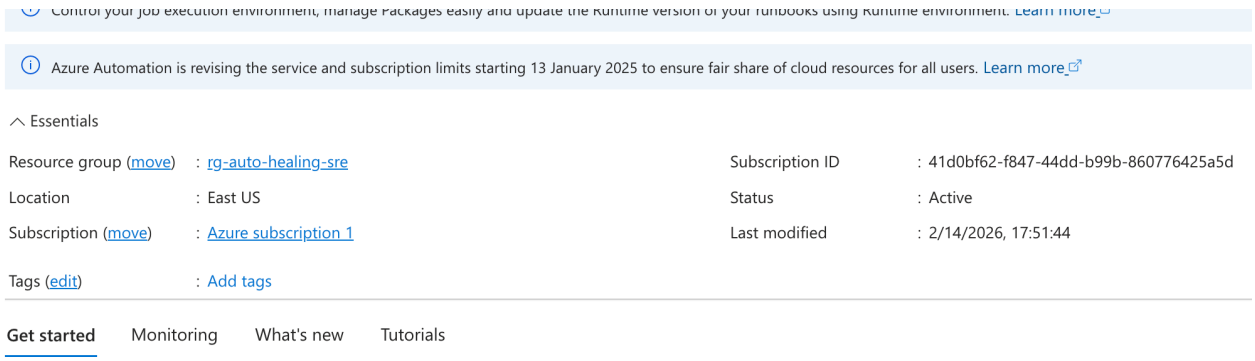
Use Managed Identities as the recommended method for authenticating with Azure
Managed identity would be more secure than Runas account since it doesn't requir
more

System assigned 

User assigned 



Once created you will see like this:

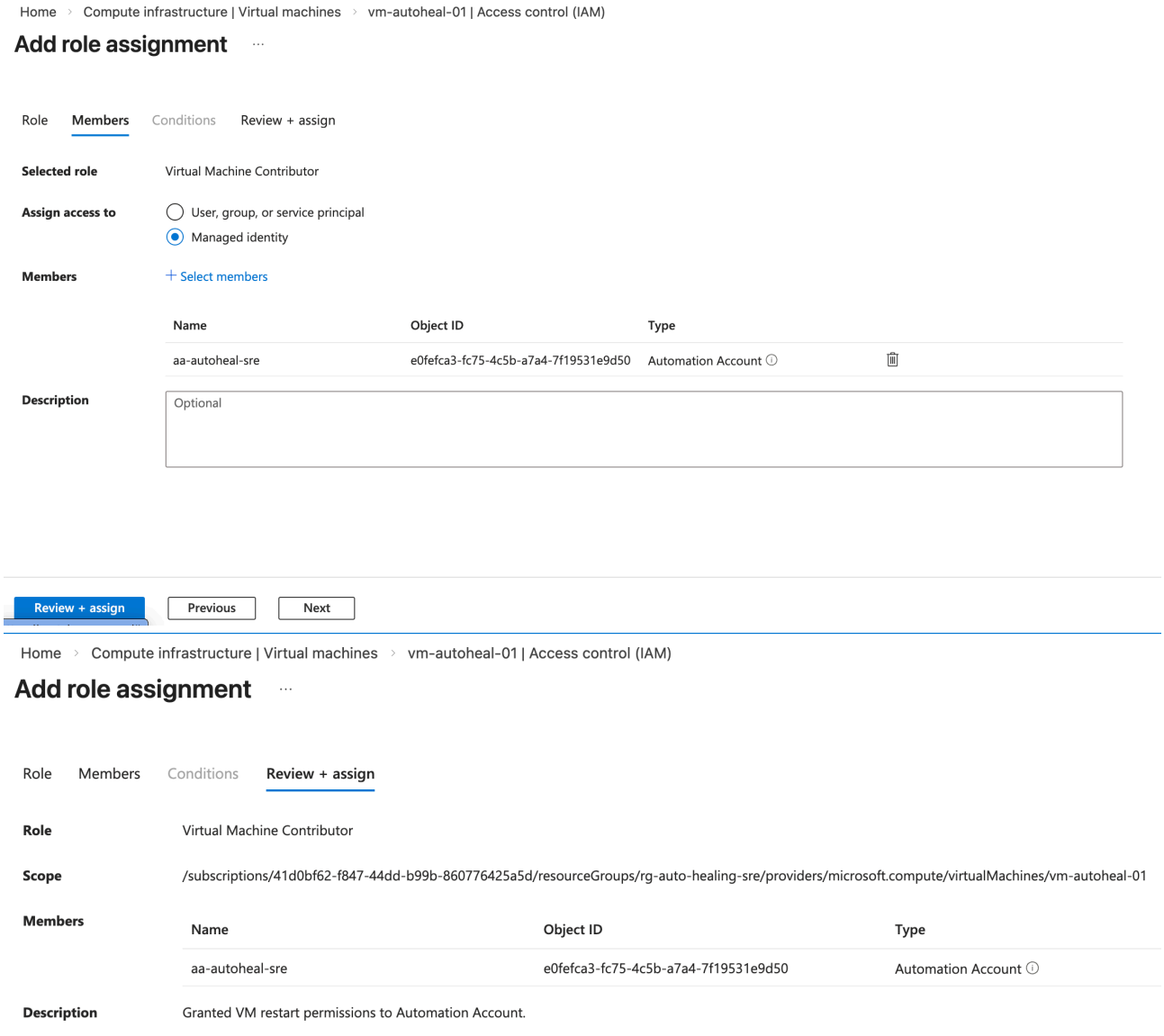


STEP 5: Give Automation Permission (CRITICAL)

1. Go to VM > **Access Control (IAM)**

2. Add role assignment
3. Role: **Virtual Machine Contributor**
4. Assign to: aa-autoheal-sre
5. Save.

Snapshot for the reference:



STEP 6: Create Runbook (Auto-Healing Logic)

1. Automation Account > **Runbooks**
2. Create Runbook

- Name: Restart-VM-Runbook
- Type: PowerShell
- Review and Create.

Select your runbaok account

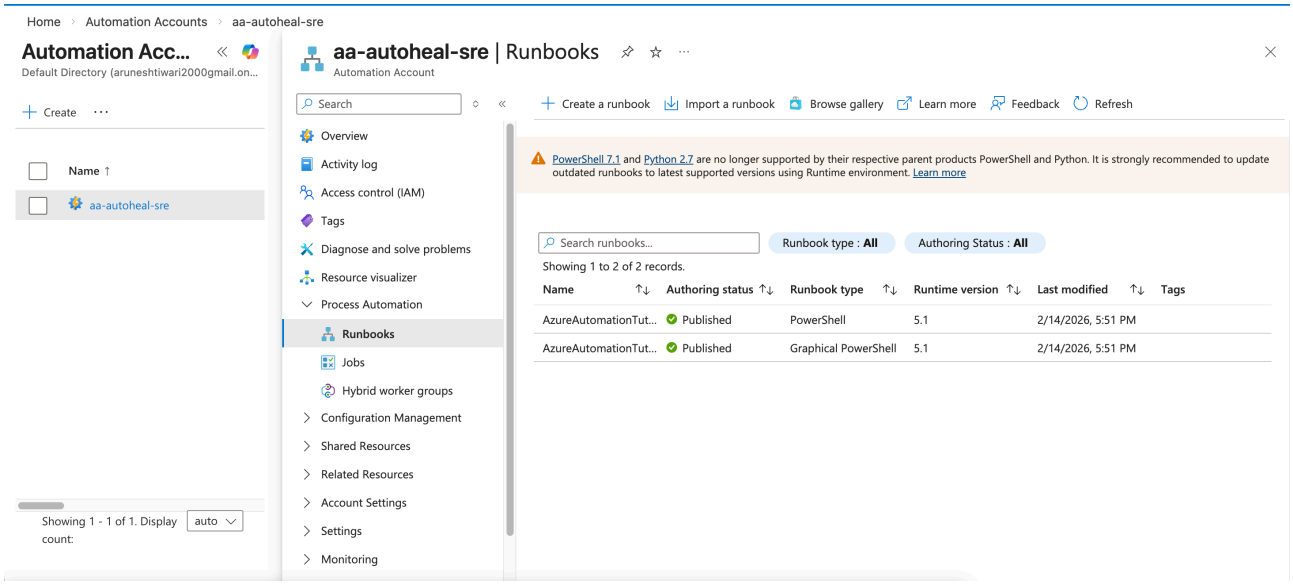
1. Paste code:

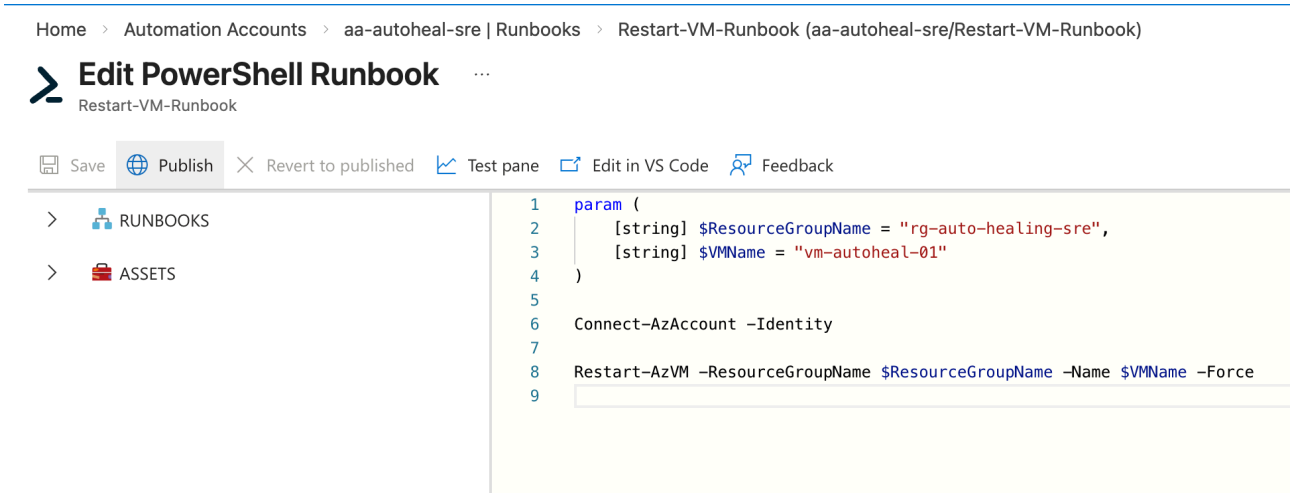
```
param (
    [string] $ResourceGroupName = "rg-auto-healing-sre",
    [string] $VMName = "vm-autoheal-01"
)

Connect-AzAccount -Identity

Restart-AzVM -ResourceGroupName $ResourceGroupName -Name $VMName
```

1. Save > Publish





STEP 7: Create Alert Rule

1. Azure Monitor > **Alerts > Create**
2. Scope: vm-autoheal-01

3. Condition:
- Metric: CPU Percentage
- Operator: Greater than
- Threshold: 80
- Duration: 5 minutes
4. Action Group > **Create New**

STEP 7.4: Action Group
In **Actions** section:
Click **Create new action group**

Creating Action Group (Inside Alert Setup)

Action Group Name: ag-autoheal
Display Name: AutoHeal

Actions Tab
1. Click **+ Add action**
2. Action type: **Automation Runbook**
3. Select:
- Subscription: your subscription
- Automation Account: aa-autoheal-sre
- Runbook: Restart-VM-Runbook
4. Leave parameters default
5. Click **OK**

Review + Create Action Group
Click **Review + Create**

STEP 7.5: Finalize Alert Rule
Back on Alert Rule page:

Alert Rule Name: cpu-high-autoheal
Severity: Sev 2
Click **Create alert rule**

Home › Monitor | Alerts

Create an alert rule ...

Signal name * ⓘ — Percentage CPU

See all signals

Alert logic

We have set the condition configuration automatically based on popular settings for this metric. Please review and make changes as needed.

Threshold type ⓘ — Static / Dynamic

Aggregation type ⓘ — Average

Value is ⓘ — Greater than

Threshold * ⓘ — 50 %

When to evaluate

Check every ⓘ — 1 minute

Lookback period ⓘ — 5 minutes

Review + create | Previous | Next: Actions >

Home › Monitor | Alerts

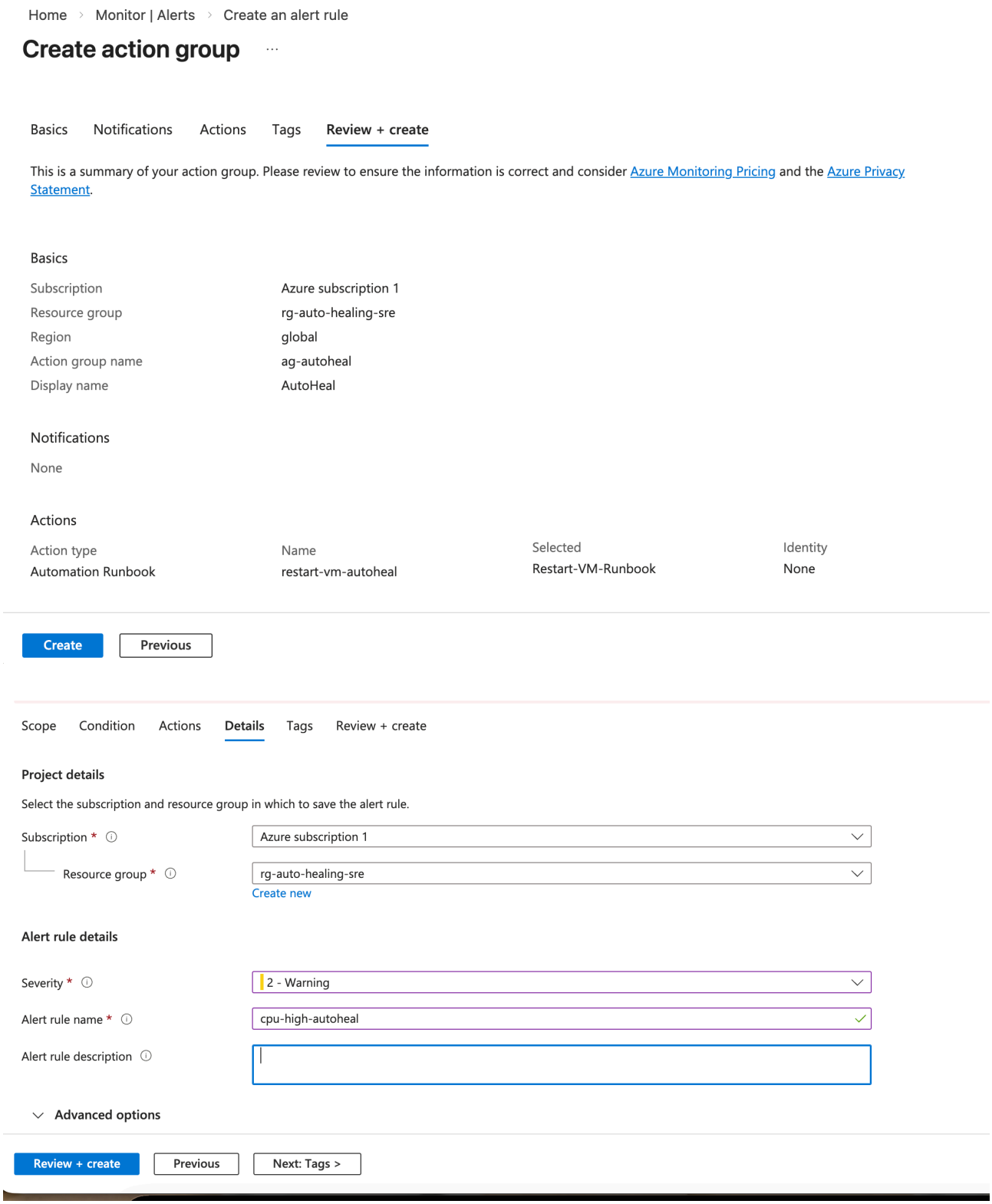
Create an alert rule ...

Scope | Condition | **Actions** | Details | Tags | Review + create

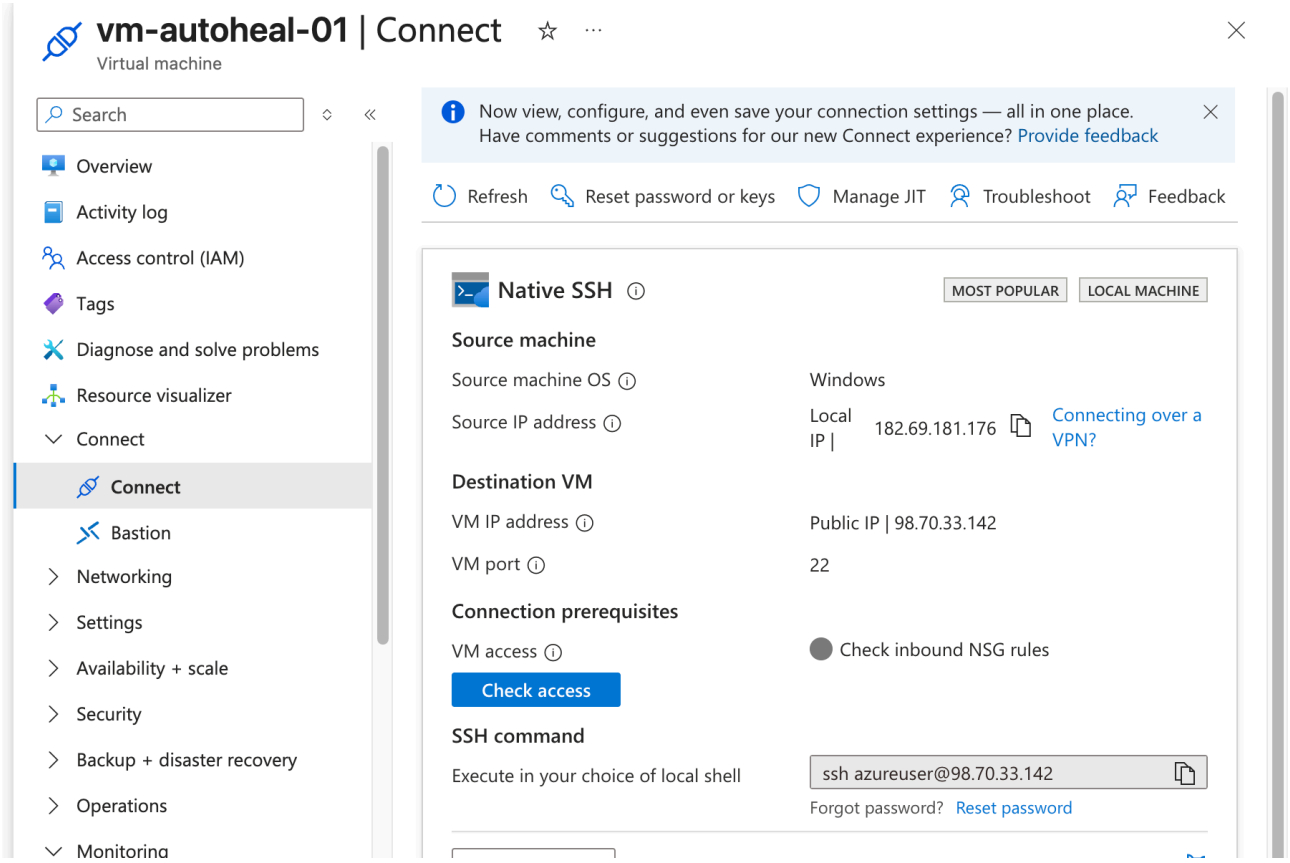
An action group is a set of actions that can be applied to an alert rule. Learn more

+ Select action groups + Create action group

Action group name	Contains actions
ag-autoheal	1 Automation Runbook



STEP 8: Test Incident
OPTION 1: SSH FROM AZURE PORTAL



You are seeing this line:

ssh azureuser@98.70.33.142

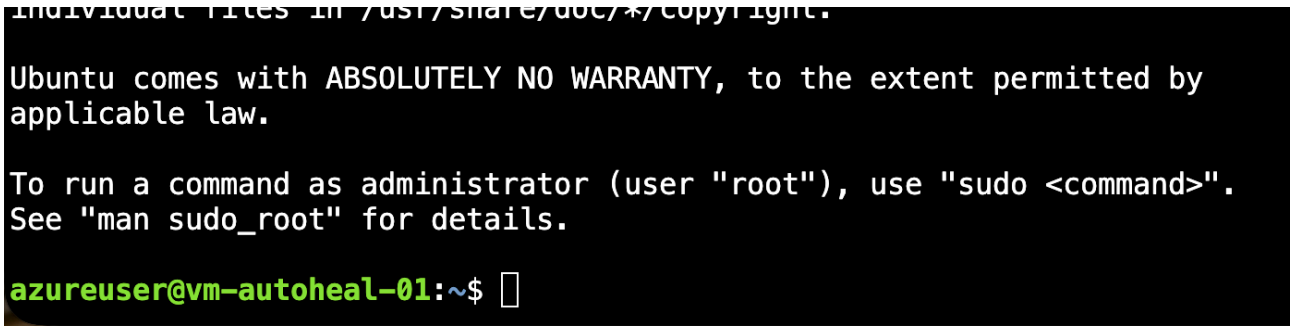
Option A

1. **Copy** the SSH command shown
2. Open **Bash in your azure portal**
3. Paste and run:

ssh azureuser@98.70.33.142

1. Type **yes** > Enter
2. Enter your VM password (you won't see typing, that's normal)

If successful, you'll see something like:



STEP 9: INSTALL STRESS TOOL (Inside VM)

Now run these commands **inside the VM**:

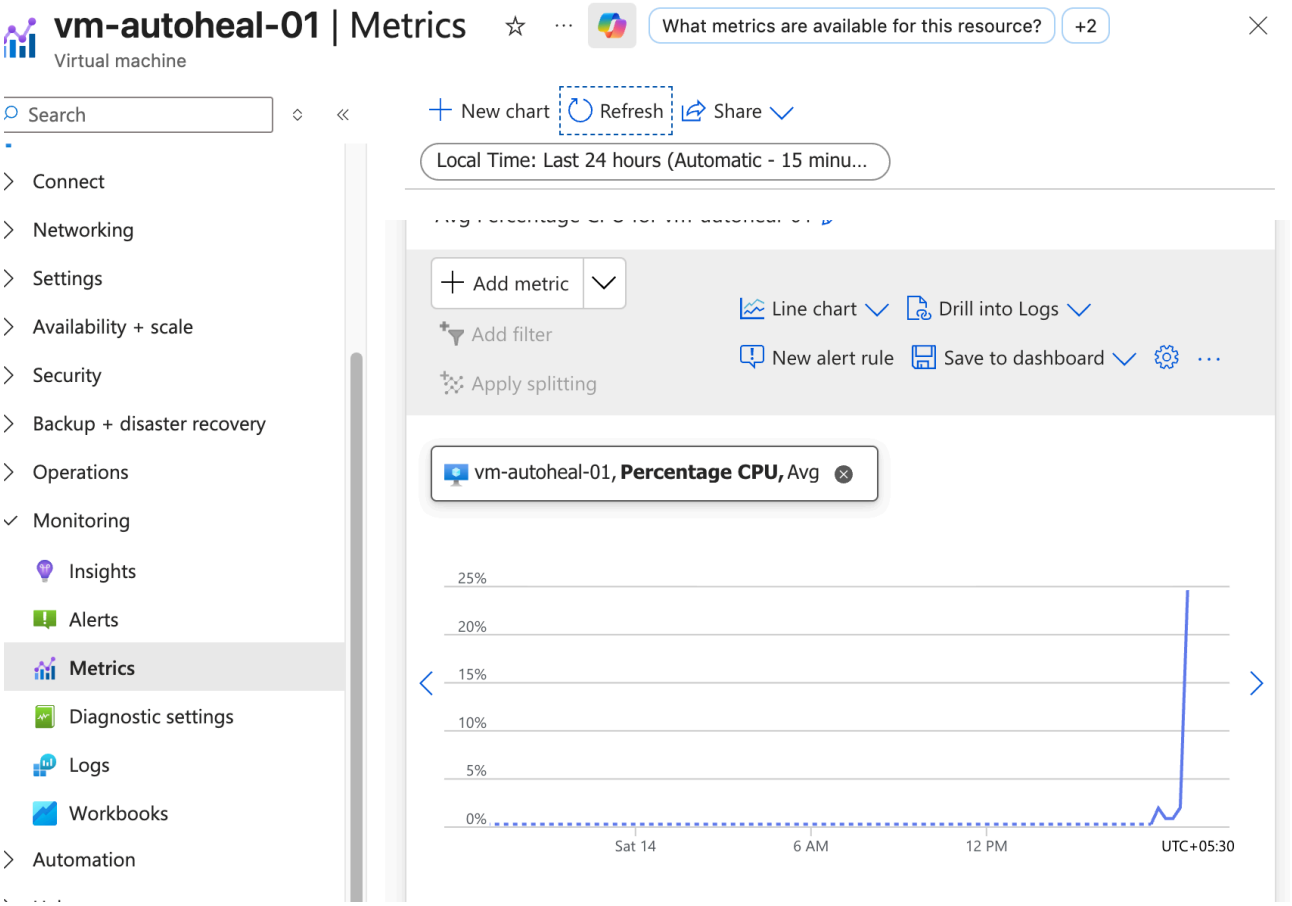
Sudo apt update
Sudo apt install stress -y

Once stress app install run this command:
stress --cpu 2 --timeout 300

NOW DO THESE CHECKS :

WAIT 2–3 MINUTES
Azure metrics + alerts are **not instant**.
Do **not** stop the stress command.

Check CPU Metric
Azure Portal > VM > Monitoring > Metrics



Set:

- **Metric**: CPU Percentage
- **Time range**: Last 30 minutes
- **Aggregation**: Average

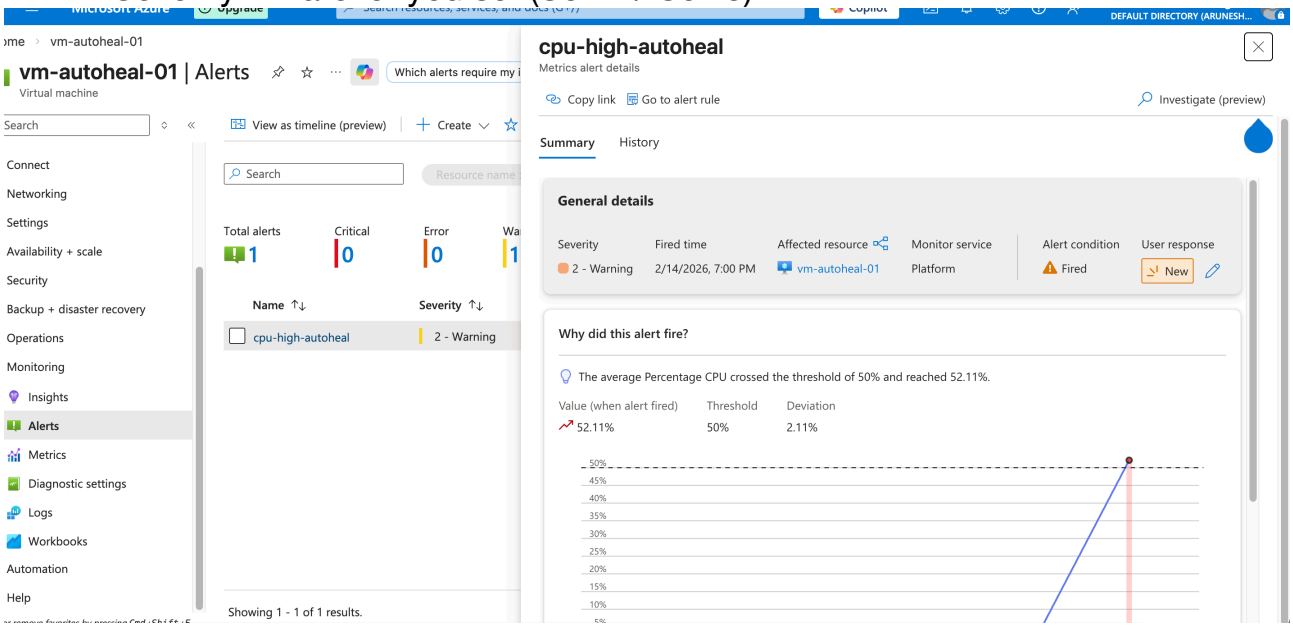
You should see CPU go **above 80%**

Check Alert Status

Azure Portal > Monitor > Alerts

You should see:

- Alert status: **Fired**
- Severity: whatever you set (Sev 2 / Sev 3)

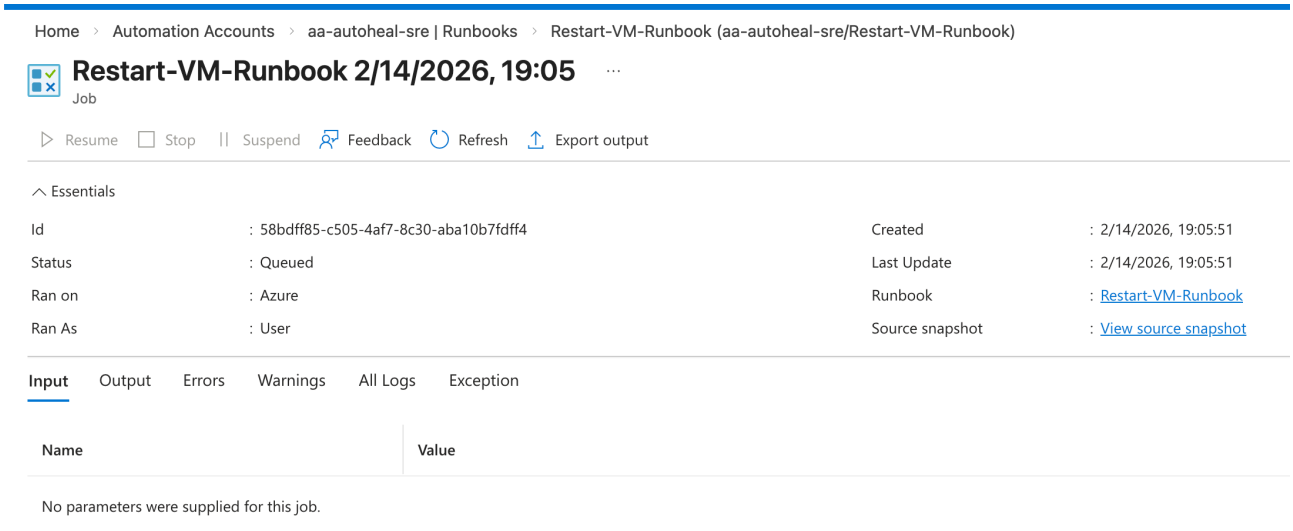


Check Runbook Execution

Automation Account > Runbooks > Restart-VM-Runbook > Jobs

Expected:

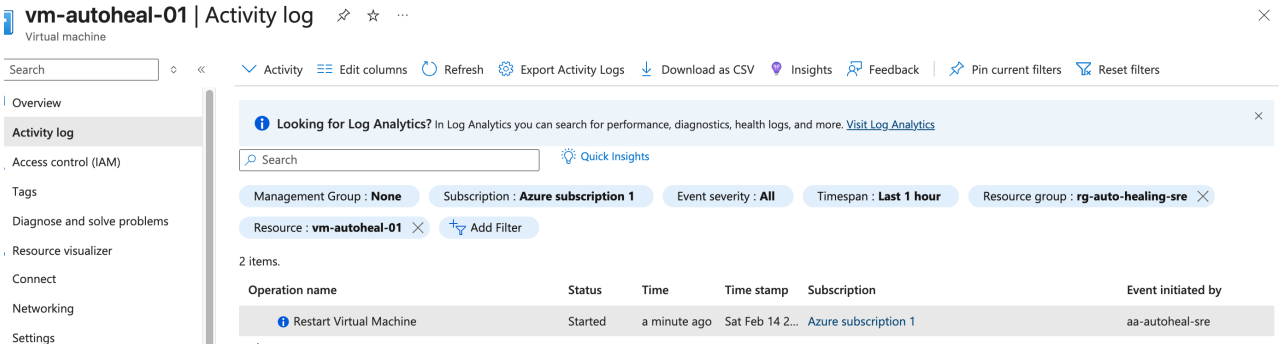
- Status: **Running > Completed**
- No red ❌ errors



Confirm VM Restart

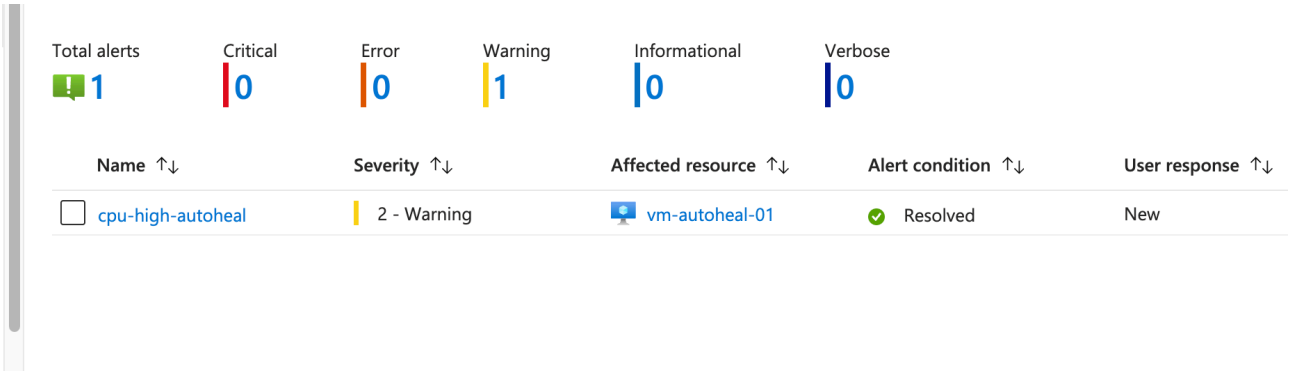
Any one of these means success:

- SSH disconnects suddenly
- VM > Overview > **Restarting**
- VM uptime resets
- You cannot SSH for 1–2 minutes



This is sign your vm restarted successfully.

Now comeback to monitor and check if incident is fired or resolved.



In my case it is resolved automatically.

STEP 10: Write Incident Postmortem

Incident Type: High CPU Usage
Detection: Azure Monitor Alert
Resolution: Auto-restart via Automation Runbook
MTTR: 3 minutes
Prevention: Auto-healing in place