

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:

[More events in the activity log →](#)

[Dismiss all](#) 

 **Deployment succeeded** 

Deployment 'CreateVm-canonical.ubuntu-24_04-lts-server-20260214172132' to resource group 'rg-auto-healing-sre' was successful.

[Go to resource](#)

 [Pin to dashboard](#)

8 minutes ago

Below Snapshot for the reference:

The screenshot shows the Azure portal interface for a virtual machine named 'vm-autoheal-01'. At the top, there's a toolbar with various actions like Connect, Start, Stop, Capture, Delete, Refresh, Scale, Open in mobile, Feedback, and CLI / PS. Below the toolbar, the 'Essentials' section provides detailed information about the VM, including its resource group ('rg-auto-healing-sre'), status ('Running'), location ('Central India (Zone 1)'), subscription ('Azure subscription 1'), and ID ('41d0bf62-f847-44dd-b99b-860776425a5d'). It also lists availability zone ('1'), operating system ('Linux (ubuntu 24.04)'), size ('Standard B2as v2 (2 vcpus, 8 GiB memory)'), primary NIC public IP ('98.70.33.142'), and other network details. The 'Tags' section shows a single tag 'Add tags'. The bottom of the page has a 'Feedback' button.

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

The screenshot shows the 'vm-autoheal-01 | Insights' page. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, and Insights. The main area displays monitoring status: 'Available' (green checkmark) and 'No outages' (green checkmark). It also shows '5 events' (yellow warning icon). Below this, there's a 'Metrics' section with a chart for 'CPU / Availability / Memory' showing 'Availability' at 0.9 and 'CPU Utilization %' at 90%. The top navigation bar includes a search bar, refresh button, resource group dropdown, Azure Monitor (selected), Diagnose And Solve Problems, and Monitor Settings. A time range selector shows 'Last 6 hours'.

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

Home > Automation Accounts

Create an Automation Account

...

[Basics](#) [Advanced](#) [Networking](#) [Tags](#) [Review + Create](#)

Create an Automation Account to hold the Automation runbooks & configuration used for automating operations and management tasks around Azure and non-Azure resources. You could execute cloud jobs in a serverless environment or use hybrid jobs on your compute via Azure Virtual machines, Arc-enabled servers or Arc-enabled VMWare VM (preview).

[Learn more](#)

Subscription * ⓘ

Azure subscription 1

Resource group * ⓘ

rg-auto-healing-sre

[Create new](#)

Instance Details

Automation account name * ⓘ

aa-autoheal-sre

Region * ⓘ

Central India

Basics **Advanced** Networking Tags Review + Create

Managed Identities

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

System assigned

User assigned

 Validation passed

Basics Advanced Networking Tags **Review + Create**

Basics

Name	aa-autoheal-sre
Subscription	Azure subscription 1
Resource group	rg-auto-healing-sre
Region	Central India

Advanced

System assigned identity	Yes
User assigned identity	None

Networking

Network connectivity	Public access
----------------------	---------------

Once created you will see like this:

 Control your job execution environment, manage packages easily and update the runtime version of your runbooks using runtime environment. [Learn more](#) 

 Azure Automation is revising the service and subscription limits starting 13 January 2025 to ensure fair share of cloud resources for all users. [Learn more](#) 

^ Essentials

Resource group (move)	: rg-auto-healing-sre	Subscription ID	: 41d0bf62-f847-44dd-b99b-860776425a5d
Location	: East US	Status	: Active
Subscription (move)	: Azure subscription 1	Last modified	: 2/14/2026, 17:51:44
Tags (edit)	: Add tags		

[Get started](#) [Monitoring](#) [What's new](#) [Tutorials](#)

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:

Home > Compute infrastructure | Virtual machines > vm-autoheal-01 | Access control (IAM)

Add role assignment ...

Name	Object ID	Type
aa-autoheal-sre	e0fefca3-fc75-4c5b-a7a4-7f19531e9d50	Automation Account ⓘ

Home > Compute infrastructure | Virtual machines > vm-autoheal-01 | Access control (IAM)

Add role assignment ...

Name	Object ID	Type
aa-autoheal-sre	e0fefca3-fc75-4c5b-a7a4-7f19531e9d50	Automation Account ⓘ

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

Name	Authoring status	Runbook type	Runtime version	Last modified	Tags
AzureAutomationTut...	Published	PowerShell	5.1	2/14/2026, 5:51 PM	
AzureAutomationTut...	Published	Graphical PowerShell	5.1	2/14/2026, 5:51 PM	

Home > Automation Accounts > aa-autoheal-sre | Runbooks > Restart-VM-Runbook (aa-autoheal-sre/Restart-VM-Runbook)

Edit PowerShell Runbook

```

1 param (
2     [string] $ResourceGroupName = "rg-auto-healing-sre",
3     [string] $VMName = "vm-autoheal-01"
4 )
5
6 Connect-AzAccount -Identity
7
8 Restart-AzVM -ResourceGroupName $ResourceGroupName -Name $VMName -Force
9

```

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**

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 ⓘ

Value is ⓘ

Threshold * ⓘ



%

When to evaluate

Check every ⓘ

Lookback period ⓘ

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

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



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-auto-healing-sre
Region	global
Action group name	ag-autoheal
Display name	AutoHeal

Notifications

None

Actions

Action type	Name	Selected	Identity
Automation Runbook	restart-vm-autoheal	Restart-VM-Runbook	None

[Create](#)[Previous](#)[Scope](#) [Condition](#) [Actions](#) [Details](#) [Tags](#) [Review + create](#)

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription * ⓘ

Azure subscription 1

Resource group * ⓘ

rg-auto-healing-sre

[Create new](#)

Alert rule details

Severity * ⓘ

2 - Warning

Alert rule name * ⓘ

cpu-high-autoheal

Alert rule description ⓘ

[Advanced options](#)[Review + create](#)[Previous](#)[Next: Tags >](#)

STEP 8: Test Incident

OPTION 1: SSH FROM AZURE PORTAL

Now view, configure, and even save your connection settings — all in one place. Have comments or suggestions for our new Connect experience? [Provide feedback](#)

Native SSH

MOST POPULAR LOCAL MACHINE

Source machine

Source machine OS: Windows

Source IP address: Local IP | 182.69.181.176 Connecting over a VPN?

Destination VM

VM IP address: Public IP | 98.70.33.142

VM port: 22

Connection prerequisites

VM access: Check inbound NSG rules

Check access

SSH command

Execute in your choice of local shell

ssh azureuser@98.70.33.142

Forgot password? [Reset password](#)

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:

```
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.

azureuser@vm-autoheal-01:~\$ []

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

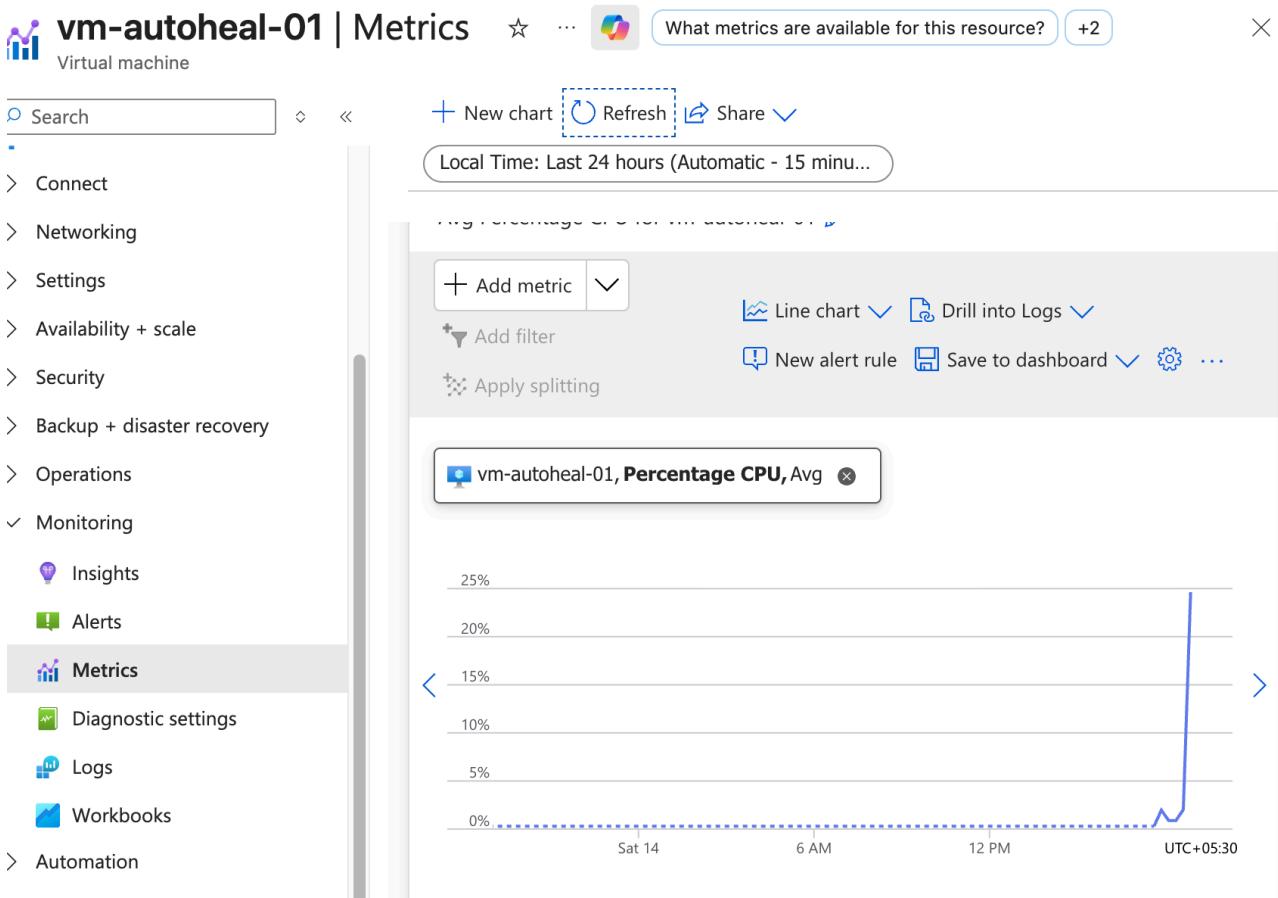
NOW DO THESE CHECKS :

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)

The screenshot shows the Azure portal interface for monitoring alerts. On the left, there's a sidebar with various monitoring options like Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, Insights, Metrics, Diagnostic settings, Logs, Workbooks, Automation, and Help. The 'Alerts' option is selected. The main area shows a list of alerts for the resource 'vm-autoheal-01'. One alert is visible: 'cpu-high-autoheal' (Severity: 2 - Warning, Fired time: 2/14/2026, 7:00 PM). A detailed view of this alert is shown on the right, including its general details (severity, fired time, affected resource, monitor service, alert condition, user response) and a chart showing CPU usage over time.

Check Runbook Execution

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

Expected:

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

The screenshot shows the execution details for a runbook named 'Restart-VM-Runbook'. The runbook was triggered on 2/14/2026 at 19:05. The status is 'Completed' with no errors. The runbook details section shows the runbook ID, status, ran on, and ran as. Below this, there are tabs for Input, Output, Errors, Warnings, All Logs, and Exception. The Input tab is selected, showing a table with columns for Name and Value. There are no parameters supplied for this job.

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

The screenshot shows the Azure Activity log for the virtual machine 'vm-autoheal-01'. The 'Activity log' tab is selected. A search bar at the top left is empty. To the right of the search bar are buttons for 'Activity', 'Edit columns', 'Refresh', 'Export Activity Logs', 'Download as CSV', 'Insights', 'Feedback', 'Pin current filters', and 'Reset filters'. Below these buttons is a message: 'Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics.' There is also a 'Quick Insights' button. Underneath this is a filter section with dropdowns for 'Management Group: None', 'Subscription: Azure subscription 1', 'Event severity: All', 'Timespan: Last 1 hour', and 'Resource group: rg-auto-healing-sre'. A 'Resource: vm-autoheal-01' is selected, and there is a 'Add Filter' button. Below the filter section, it says '2 items.' and lists one item: 'Restart Virtual Machine' with status 'Started', time 'a minute ago', timestamp 'Sat Feb 14 2...', subscription 'Azure subscription 1', and initiated by 'aa-autoheal-sre'.

This is sign your vm restarted successfully.

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

The screenshot shows the Azure Monitor Alerts page. At the top, there are six summary metrics: 'Total alerts' (1), 'Critical' (0), 'Error' (0), 'Warning' (1), 'Informational' (0), and 'Verbose' (0). Below these are five filter buttons: 'Name ↑↓' (cpu-high-autoheal), 'Severity ↑↓' (2 - Warning), 'Affected resource ↑↓' (vm-autoheal-01), 'Alert condition ↑↓' (Resolved), and 'User response ↑↓' (New). The main table displays one alert row: 'cpu-high-autoheal' (Severity: 2 - Warning, Affected resource: vm-autoheal-01, Alert condition: Resolved, User response: New).

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