OpsAtlas
OPERATIONAL RUNBOOKS BY SMALLWOOD ENTERPRISES
Reliable cloud operations documentation

Azure VM Down or Unreachable

Azure Troubleshooting Runbook 01

Azure Troubleshooting Runbooks

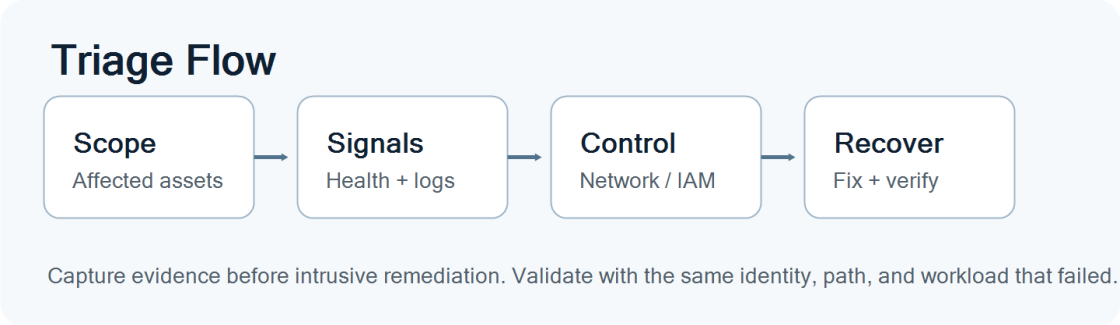
2026-05-29

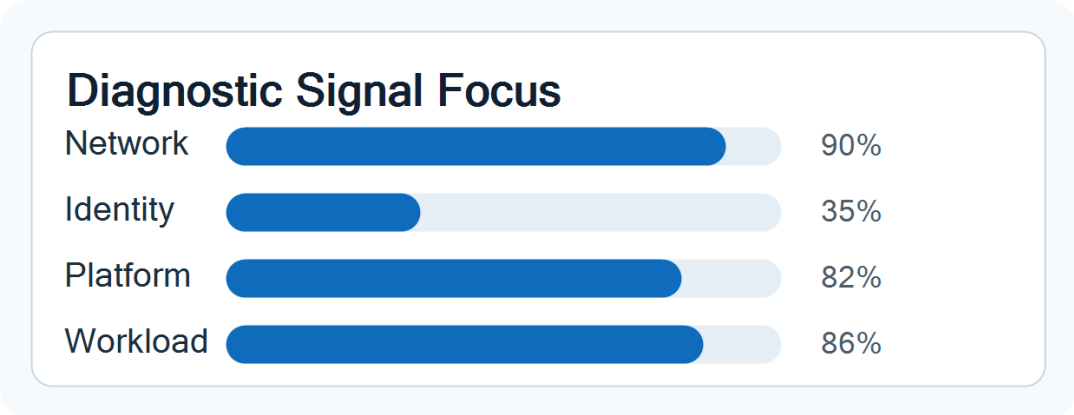
Table of Contents

Azure VM Down or Unreachable

Audience: Cloud administrators, help desk escalation engineers, MSP NOC teams
Severity guide: Sev 1 when production service is unavailable; Sev 2 when one host is impaired but redundant capacity is healthy.
Incident objective: Determine whether the VM is stopped, platform-impaired, network-isolated, guest-OS hung, or application-down, then restore safe access without destroying evidence.

> **Operator note:** Start with evidence capture and scope control. Make the smallest reversible change that restores service, then replace emergency access or broad permissions with a durable fix.





Common Symptoms

- Azure portal shows the VM as unavailable, stopped, failed, or running but users cannot reach it.
- RDP, SSH, HTTP, or application probes time out.
- Monitoring shows guest heartbeat loss, failed connection tests, or abrupt CPU/network drop.
- Service owners report a brownout after a change, patch, resize, redeploy, or network update.

First 15 Minutes

- Confirm scope: single VM, availability set, VMSS instance, subnet, region, or dependency.
- Check Resource Health and Activity Log for host events, user actions, deallocations, failed extensions, or resize operations.
- Verify power state, provisioning state, boot diagnostics screenshot, serial console, and guest heartbeat.
- Run Network Watcher connection troubleshoot from a known source to the VM IP and expected port.
- Review NIC effective routes and effective NSG rules before changing security rules.
- If the VM runs a critical workload, snapshot OS/data disks before intrusive repair.

Command Starters

Replace placeholders such as <rg>, <vm>, <ns>, and <resourceId> before running. Use Azure Cloud Shell or a workstation with the right Azure CLI, kubectl, and PowerShell context.

```
az vm get-instance-view -g <rg> -n <vm> --query "{power:instanceView.statuses[?starts_with(code,'PowerState/')].displayStatus|[0],provisioning:provisioningState}" -o table

az vm boot-diagnostics get-boot-log -g <rg> -n <vm>

az network watcher test-connectivity --source-resource <sourceVmId> --dest-address <privateIp> --dest-port <port>

az network nic list-effective-nsg -g <rg> -n <nicName> -o table

az network nic show-effective-route-table -g <rg> -n <nicName> -o table
```

Decision Path

If you find...	Do this next
VM not running or deallocated	Start the VM, confirm auto-shutdown or automation did not stop it, and review cost/schedule runbooks.
Boot diagnostics shows OS boot failure	Use serial console, repair VM, or disk-swap recovery. Preserve snapshots before repair.
Connectivity blocked by NSG/UDR/firewall	Fix the most specific blocking control first; document before/after rule evidence.
Guest is running but service is down	Move to application service checks: listener, process, dependency, certificate, disk, and logs.
Resource Health reports platform issue	Fail over if designed, open support case, and attach Resource Health evidence.

Remediation Actions

- Restart only after capturing boot diagnostics, guest logs, and Activity Log evidence unless the business owner approves immediate recovery.
- For Windows access repair, reset RDP configuration or local admin password using VM access tooling.
- For Linux access repair, reset SSH configuration or user credentials with the VMAccessForLinux extension.
- If the host is unhealthy and disks look intact, redeploy the VM to a new Azure host.
- If network path is blocked, apply a temporary just-in-time allow rule scoped to the operator source IP, then replace with the permanent rule.

Validation Checklist

- RDP/SSH or service probe succeeds from the approved source network.
- Azure Monitor heartbeat, CPU, disk, and network metrics return to normal.
- Application owner confirms service-level validation, not only VM login.
- Temporary emergency rules, test VMs, and broad permissions are removed.

Escalation Triggers

- Boot diagnostics indicates disk corruption, repeated kernel panic, or Windows recovery loop.
- Resource Health shows an Azure platform event affecting protected workloads.
- Multiple VMs in different subnets fail at the same time, suggesting shared DNS, firewall, route, or identity dependency.

Evidence to Attach

- Incident start time, detection source, affected resource IDs, subscription, region, and business owner.
- Exact error text, request IDs, correlation IDs, client IPs, and timestamps in UTC.
- Before/after screenshots or command output for health, routes, security rules, diagnostics, and logs.
- Change record for any emergency rule, role assignment, restart, redeploy, rollback, or scale action.

Customer-Facing Summary Template

What happened: `<brief customer-safe description>`
Impact: `<users/services/regions affected and time range>`
Root cause: `<confirmed root cause or current leading cause>`
Resolution: `<fix applied and validation completed>`
Prevention: `<monitoring, guardrail, policy, or architecture follow-up>`

Reference Anchors

- Troubleshoot RDP connections to an Azure VM
- Troubleshoot SSH connections to an Azure Linux VM
- Troubleshoot application connectivity on Azure VMs