OpsAtlas
OPERATIONAL RUNBOOKS BY SMALLWOOD ENTERPRISES
Reliable cloud operations documentation

OCI Compute Instance Unreachable

Oracle Cloud Troubleshooting Runbook 01

Oracle Cloud Troubleshooting Runbooks

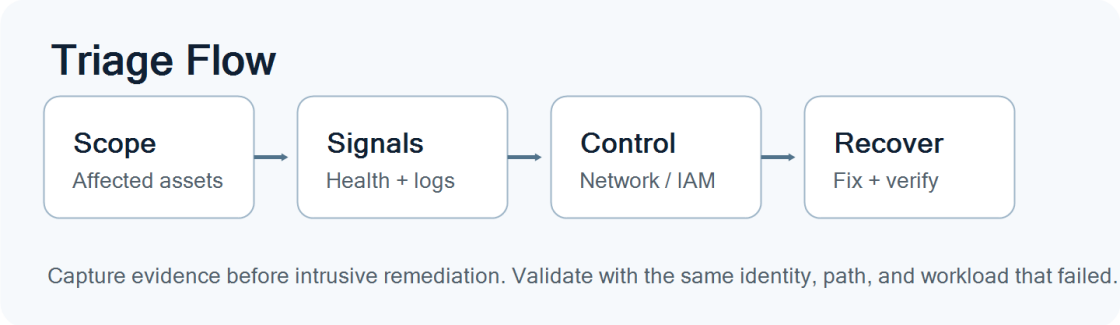
2026-05-29

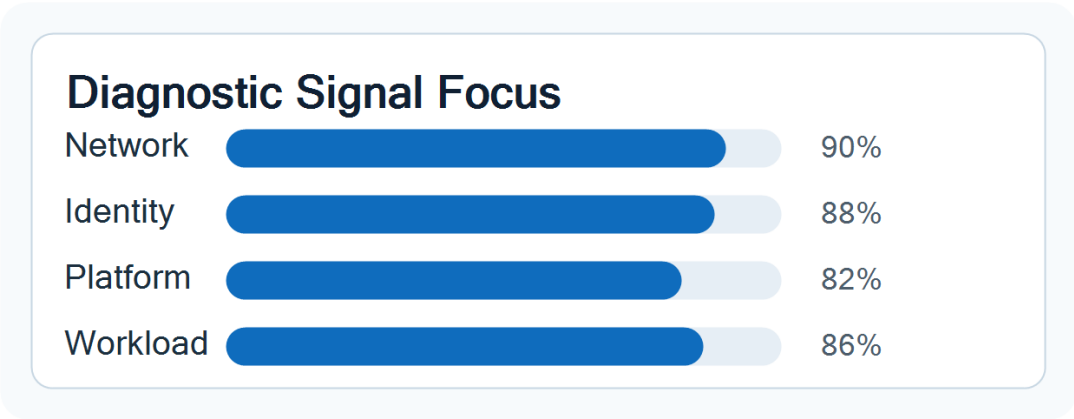
Table of Contents

OCI Compute Instance Unreachable

Oracle Cloud Troubleshooting Runbook 01
Audience: Cloud administrators, SREs, support personnel, and MSP escalation teams
Severity guide: Sev 1 when production access, customer traffic, identity control, or protected data recovery is blocked; Sev 2 when impact is partial or a workaround exists.
Incident objective: Restore administrative or application access by isolating instance lifecycle state, boot health, VNIC attachment, route rules, security lists, NSGs, public/private addressing, and guest OS listener failures.

> **Operator note:** Capture OCIDs, compartments, regions, request IDs, timestamps, and before/after configuration evidence. Prefer the smallest reversible change that restores service, then replace emergency access with a durable fix.





Common Symptoms

- SSH, RDP, HTTP, or application probes time out.
- Instance shows running but console connection, serial console, or service access fails.
- Access broke after patching, shape change, image change, security-list update, or route change.

First 15 Minutes

- Confirm instance lifecycle state, availability domain, fault domain, compartment, image, shape, and recent work requests.
- Review console history, boot volume health, serial console output, and instance metrics.
- Validate VNIC private/public IPs, subnet route table, security list rules, NSGs, and internet/NAT/service gateway path.
- Check whether the target service is listening inside the guest OS and whether host firewall rules allow it.
- Create a boot volume backup before invasive repair or boot-volume swap recovery.

Command Starters

Replace placeholders before running. Use the correct OCI profile, region, compartment, tenancy, and principal. Record output in the incident ticket.

```
oci compute instance get --instance-id <instance-ocid>

oci compute instance list-vnics --instance-id <instance-ocid>

oci compute console-history capture --instance-id <instance-ocid> --display-n
ame incident-console-history

oci network vnic get --vnic-id <vnic-ocid>

oci network subnet get --subnet-id <subnet-ocid>
```

Decision Path

If you find...	Do this next
Instance not running	Start the instance and check scheduled automation, capacity, quotas, and work request failures.
Boot/guest failure	Use serial console or boot-volume recovery after preserving evidence.
Network path blocked	Fix the most specific route rule, security list, NSG, gateway, or host firewall control.
Host reachable but app down	Move to process, listener, dependency, certificate, disk, and application log checks.

Remediation Actions

- Use Bastion or serial console for emergency access instead of opening SSH/RDP broadly.
- Revert broad security-list or NSG emergency rules after durable access is restored.
- Recover through boot-volume detach/attach only after backing up the affected volume.
- Redeploy or rebuild from image/backup if instance metadata and boot evidence indicate corruption.

Validation Checklist

- SSH/RDP or service probe succeeds from the approved source network.
- Instance metrics and guest logs show stable boot and service health.
- Temporary public IPs, emergency rules, and break-glass access are removed.

Evidence to Attach

- Tenancy OCID, compartment OCID, region, affected resource OCIDs, request IDs, and UTC timestamps.
- Audit, work request, service event, health, metrics, logs, or backend status evidence.

- Before/after IAM policy, route table, security rule, DNS, health check, or service configuration.
- Approval record for any emergency permission, public exposure, route, restart, failover, replay, rollback, or destructive repair.

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, IaC, policy, or architecture follow-up>`

Reference Anchors

- Troubleshooting instances
- Connecting to an instance
- Instance console connections