Description:
This runbook is used when a compute or worker node has an availability less than 98 percent over a set period (24 hours, 7 days, etc). This usually means the node was down, restarted often, or was otherwise unavailable.

Steps to Follow:

Step 1: Check the Alert
- Confirm the alert details
- Note the node name, instance ID, and time window
- Confirm it is not a false alarm

Step 2: Check Node Metrics
- Use monitoring dashboard or command line to check availability over time
- Example command : oci monitoring metric-data summarize-metrics-data --namespace oci_computeagent --query-text "Availability[1h].mean()" --resource-id <instance_id> --start-time <start_time> --end-time <end_time>

Step 3: Check for Restarts or Failures
- Check if the node was restarted or terminated recently
- Use console or CLI
- Example command : oci compute instance get --instance-id <instanced>

Step 4: Log Into the Node
- SSH into the node if it's up
- Example : ssh opc@<node_ip>
- Check uptime : uptime
- Check logs : dmesg | tail -n 50 journalctl -xe

Step 5: Look for Resource Issues
- Check CPU and memory : top
- Check disk space: df -h
- Check failed services: systemctl --failed

Step 6: Check if Node Is in a Group
- If it's in a node pool or instance group, check if auto-replacement worked
- Check with : oci compute instance list --compartment-id <compartment_id>
- Or use orchestrator like Kubernetes : kubectl get nodes

Step 7: Replace or Restart Node If Needed
- If the node is unhealthy, consider replacing or restarting it
- Restart command : oci compute instance action --instance-id <instance_id> --action RESET
- In Kubernetes : kubectl cordon <node_name> kubectl drain <node name> --ignore-daemonsets --delete-emptydir-data

Step 8: Notify Teams
- Share what you found in the SRE or infra channel
- Example message : Node <node_name> had low availability due to repeated reboots. Restarted and stable now.

Step 9: Monitor for Stability

- Keep an eye on metrics for next 30 minutes to 1 hour
- Make sure availability improves
- Ensure alert clears on its own or manually mark as OK if resolved

Step 10: Document the Incident

- Record what happened, root cause, and what was done
- Save in your incident tracker or ticketing system