SAMPLE ASSESSMENT

Infrastructure Assessment Report

OpsMate by Triont · triont.com.au

Sample assessment combining findings from multiple production AWS environments.

Download PDF ↓

Account scope	Single Account
Region	ap-southeast-2 (Sydney)
Access level	Read-only IAM role
Assessment date	February 2026
Classification	SAMPLE — composite data from multiple assessments

Executive Summary

OpsMate performed an AI-driven contextual discovery of a single AWS account responsible for network ingress — routing external traffic from global IoT devices and partners to backend processing systems. This is not a checkbox compliance scan. OpsMate explores your infrastructure the way a senior engineer would, following relationships between resources and identifying patterns that automated scanners miss.

In a single read-only pass, OpsMate discovered:

10	**152**	**88**	**58%**
LOAD BALANCERS	TARGET GROUPS	UNHEALTHY TARGETS	FAILURE RATE

🟥 Critical Finding: IoT Device Connectivity at Risk

88 of 152 target groups (58%) have no healthy targets. These target groups serve IoT device hub endpoints across global locations including Ireland, New Zealand, Portugal, Australia, UAE, and West Africa.

All unhealthy target groups trace back to just 3 backend EC2 instances with consistently failing health checks. If any of these instances fail, connectivity to field devices across multiple international sites would be lost simultaneously with no automated failover.

What this means for your business

This isn't a theoretical risk. The infrastructure currently serving global IoT traffic has a 58% unhealthy rate across its target groups, concentrated on a small number of backend instances. A single instance failure could cascade into loss of telemetry from dozens of field devices across multiple countries — potentially affecting operations, SLAs, and regulatory reporting.

> *This is the kind of finding that typically surfaces when customers notice — not when engineering teams catch it. OpsMate found it in one automated pass.*

Discovery Detail

OpsMate mapped the complete ingress topology from internet-facing load balancers through to backend targets, including listener configurations, port mappings, and health status.

Load Balancer Overview

Name	Type	Scheme	AZs	Listeners
Port Forwarder NLB	NLB	Internet-facing	1 AZ	32
FTP Gateway NLB	NLB	Internet-facing	3 AZs	24
Service NLB (public)	NLB	Internet-facing	3 AZs	3
Application ALB	ALB	Internet-facing	3 AZs	2
Device NLB — AZ-A	NLB	Internet-facing	1 AZ	28
Device NLB — AZ-B	NLB	Internet-facing	1 AZ	28
Internal Service NLB	NLB	Internal	3 AZs	3
Internal Application ALB	ALB	Internal	3 AZs	3
VPN Endpoint NLB	NLB	Internal	2 AZs	1
Backend Service NLB	NLB	Internal	1 AZ	1

Target Group Health Analysis

OpsMate didn't just count unhealthy targets — it traced the pattern. The 88 unhealthy target groups aren't 88 independent problems. They cluster into three root causes:

HIGH **IoT Hub Instance (single point of failure)**

24 target groups across global locations all route to one instance with failed health checks. Covers Ireland, NZ, Portugal, Australia, UAE, and West Africa.

Single instance failure = global telemetry loss

HIGH **Device Gateway Instances (2 instances, ~46 target groups)**

Two EC2 instances serving device-specific target groups across two availability zones. Both showing failed health checks. Pattern suggests a systemic issue rather than isolated service failures.

Systemic failure pattern — not isolated incidents

MEDIUM **Legacy / unused target groups**

Several target groups appear unused or orphaned, including one with no registered targets at all. These add operational noise and make it harder to identify genuine issues.

Increases MTTR during incidents

Compute Fleet Summary

13 EC2 instances identified across the account. Instance types range from t3.nano to m5.xlarge. One instance has been running since August 2023 without replacement — potential patching and lifecycle management concern. Mix of Amazon Linux 2, Amazon Linux 2023, and Ubuntu AMIs.

Recommendations

Prioritised and actionable — every recommendation includes effort estimates and deferral risk.

1

HIGH

Investigate IoT hub health check failures

The single instance serving 24 global hub target groups has consistently failing health checks. Determine if this is a misconfiguration or genuine service degradation.

Estimated effort: 2–4 hours | Risk if deferred: potential global telemetry loss

2

HIGH

Assess device gateway redundancy

Two instances serving ~46 device target groups are both unhealthy. Review whether these need replacement, scaling, or architectural redesign for proper failover.

Estimated effort: 1–2 days | Risk if deferred: device connectivity outage with no failover

3

MEDIUM

Clean up orphaned target groups

Remove or decommission unused target groups to reduce operational noise. At least one has no registered targets at all.

Estimated effort: 2–4 hours | Risk if deferred: increased MTTR during incidents

4

MEDIUM

Review single-AZ load balancer deployments

Two internet-facing NLBs are deployed in a single availability zone, creating an AZ-level single point of failure.

Estimated effort: 4–8 hours | Risk if deferred: AZ failure causes full service disruption

5

LOW

Instance lifecycle and patching review

One instance has been running since August 2023. Review AMI currency, patch levels, and whether replacement with a current AMI is warranted.

Estimated effort: 1–2 hours | Risk if deferred: increasing security exposure over time

What happens next

This sample covers a single account, single pass. A full OpsMate engagement includes:

- All AWS accounts in your organisation scoped and assessed
- Weekly automated reports delivered to your preferred channel
- Interactive AI-powered chat for follow-up questions about your environment
- Remediation guidance broken into scoped, actionable work items
- Trend tracking — is your environment getting better or worse over time?

Download PDF ↓

This is a sample report for demonstration purposes. Data points and metrics are generalised from multiple real OpsMate assessments across different production AWS environments. Account identifiers, instance IDs, and specific infrastructure details have been anonymised.