Infrastructure Health Report

Account: sandbox (471000000001) | Customer: meridian-logistics-a1b2c3d4 | Date: 2026-04-15

Overall Status

AMBER

Executive Summary

This week's sandbox health report is AMBER. There are no critical findings, but four warnings have been open since the initial scan on 1 April 2026 and remain unaddressed. The most significant issues are the absence of CloudTrail (no audit trail for developer activity), an unconfigured IAM password policy, and 8 EC2 instances running around the clock with no schedule — costing an estimated $520/month that could be eliminated with instance scheduling. A new EC2 instance was added on Friday, increasing the account cost from $867 to $1,207/month. No security incidents detected.

Critical Findings

No critical findings.

Warnings

1. IAM password policy not configured

GetAccountPasswordPolicy returns a NoSuchEntityException — no account-level password policy exists. Developers can set passwords of any length with no complexity or rotation requirements. Open since initial scan 1 April 2026.

Impact: Weak developer credentials increase the risk of account compromise via credential stuffing or password guessing. The sandbox account shares the same AWS Organisation as production — a compromised sandbox account can be used as a pivot point to attempt lateral movement to other accounts.

Action: Apply an IAM password policy via Console (IAM !Account settings) or CLI: minimum 14 characters, require uppercase, lowercase, numbers and symbols, 90-day maximum age, prevent reuse of last 5 passwords. Takes effect immediately for all new password changes.

2. CloudTrail not enabled — no audit trail for developer activity

DescribeTrails returns an empty trail list for ap-southeast-2. All developer API activity — IAM changes, EC2 launches, S3 access, security group modifications — is occurring without any log. Open since initial scan 1 April 2026.

Impact: If a developer accidentally deletes a resource, misconfigures an IAM policy, or introduces a security issue, there is no way to determine when it happened, what changed, or who made the change. In the event of a security investigation, the absence of CloudTrail logs is a significant gap.

Action: Enable a multi-region CloudTrail trail via Console or CLI. Configure log delivery to an S3 bucket with MFA delete and SSE enabled. Enable CloudWatch Logs integration for real-time alerting on sensitive API calls (e.g., DeleteBucket, CreateUser, AttachUserPolicy). Estimated monthly cost for a low-activity sandbox: ~$2.

3. 8 EC2 instances running 24/7 — estimated $520/month avoidable spend

Instances i-dev-001 through i-dev-008 (mix of t3.medium and t3.large) have been running continuously since their launch dates, ranging from 18 to 47 days ago. No Instance Scheduler tags (schedule, aws:autostop, or similar) were detected. A new instance (i-dev-008, t3.large) was added on 2026-04-11. Open since initial scan 1 April 2026.

Impact: Development instances are typically used 8–10 hours per weekday. Running them 24/7 means approximately 75% of runtime is idle spend. At current instance mix, stopping instances outside business hours (Mon–Fri 8am–6pm AEST) would save an estimated $520/month — $6,240/year.

Action: Apply AWS Instance Scheduler or use EventBridge Scheduler to power down instances outside business hours. Alternatively, tag instances with a schedule tag and use the AWS Instance Scheduler CDK construct. A simpler immediate fix: instruct developers to stop instances at end of day and add a Lambda/EventBridge rule to force-stop any running dev instances at 7pm AEST daily.

4. No AWS Budgets configured — cost spikes go undetected

DescribeBudgets returns no budgets for this account. The account cost increased from $867 to $1,207 this week (a 39% increase) following a new EC2 instance launch with no notification triggered. Open since initial scan 1 April 2026.

Impact: Developers can launch high-cost resources — GPU instances, Redshift clusters, NAT Gateways — and the cost will only be discovered at month end. There is no guardrail between a developer experimenting and an unexpected $10,000 bill.

Action: Create a monthly budget of $1,500 with email alerts at 80% ($1,200) and 100% ($1,500). Add a second alert at 120% to catch runaway spend. Use aws budgets create-budget or the AWS Console (Billing !Budgets !Create budget). Takes 5 minutes to configure.

Cost Summary

Estimated 30-day total: $1207.00

Service	30-day Cost
EC2	$930.00
S3	$130.00
RDS	$90.00
Lambda	$40.00
CloudWatch	$17.00

Recommendations

[MEDIUM] 1. Enable CloudTrail immediately
No audit trail exists for developer activity. ~$2/month. Required for any meaningful security posture in a cloud account — even a sandbox.

[MEDIUM] 2. Schedule dev instances to stop outside business hours
8 instances running 24/7. Estimated saving: $520/month ($6,240/year). Use EventBridge Scheduler or Instance Scheduler tags.

[MEDIUM] 3. Configure IAM account password policy
No minimum password requirements. Apply 14-char minimum, complexity, 90-day rotation. Takes 5 minutes via IAM console.

[LOW] 4. Set up AWS Budgets alert
No cost guardrails in place. Create a $1,500/month budget with alerts at 80% and 100%. The account grew 39% in one week without any notification.

This report was generated using read-only AWS API access. No changes were made to your infrastructure. For support, contact support@triont.com.