Infrastructure Health Report

Account: production (471000000004) | Customer: meridian-logistics-a1b2c3d4 | Date: 2026-04-15

Overall Status

RED

Executive Summary

This week's production health report is RED. Two issues require immediate attention: an ACM certificate expiring in 11 days that will take the customer-facing application offline if not renewed, and a PostgreSQL database port exposed to the public internet — a critical security exposure that has been open since 22 March with no remediation. Three additional warnings remain open from last week. The only change since the previous report is that RDS storage has grown from 83% to 87% utilisation, increasing the urgency of enabling autoscaling. Estimated monthly cost is $9,240, up $110 from last week. No new instances or services were detected.

Critical Findings

1. ACM certificate expires in 11 days — auto-renewal not enabled

The TLS certificate for app.meridianlogistics.com.au expires on 2026-04-26. Certificate was issued 2025-04-26 for a 12-month term. DNS validation is configured but auto-renewal has not been enabled in ACM — the certificate will not renew automatically. First flagged last week at 18 days remaining; now 11 days.

Impact: When the certificate lapses, all HTTPS traffic to the customer-facing application will fail immediately. Browsers will show a security warning and block access by default. Modern browsers typically begin showing 'Not Secure' warnings 3 days prior to expiry. This will affect all users of the platform and is likely to generate support calls within hours.

Action: In the AWS Console, open ACM !Certificates !select the certificate !Actions !Renew. Enable DNS auto-renewal so this cannot recur. If Route 53 hosts the domain, ACM can add the validation CNAME automatically. Estimated fix time: 20 minutes.

2. PostgreSQL port 5432 open to the public internet

Security group sg-0a4f2c1d (attached to ml-prod-pg-primary) has an inbound rule allowing TCP 5432 from 0.0.0.0/0 and ::/0. This security group is attached to the primary RDS instance. Open since 22 March 2026 — present in the last three weekly reports with no action taken.

Impact: The production PostgreSQL database is directly reachable from anywhere on the internet. Automated scanners routinely probe port 5432 and attempt credential attacks. A single weak or reused password on any database user could result in a full data breach. This is the highest-risk finding in the account.

Action: Remove the 0.0.0.0/0 inbound rule from sg-0a4f2c1d. Add a replacement rule allowing TCP 5432 only from the application subnet CIDR (e.g., 10.0.1.0/24). No downtime is required — RDS security group changes apply immediately. Verify using: aws ec2 describe-security-groups --group-ids sg-0a4f2c1d.

Warnings

1. RDS storage at 87% — autoscaling disabled

ml-prod-pg-primary (db.r6g.2xlarge, 500 GB gp3) is using 435 GB (87%). Storage was at 83% last week — growing at approximately 10 GB/week. RDS storage autoscaling is not enabled. When storage reaches 100% the instance will transition to read-only mode and refuse all write operations.

Impact: At the current growth rate, the database will exhaust storage in approximately 6–7 weeks. RDS will not self-recover from a full-storage event — manual intervention is required, which typically takes 30–60 minutes during which the application cannot write any data.

Action: Enable RDS storage autoscaling with a maximum threshold of 1,000 GB (via Console: RDS !Databases !ml-prod-pg-primary !Modify !Storage autoscaling). This takes effect within minutes with no downtime. As a secondary measure, investigate what is driving the 10 GB/week growth — check table sizes using SELECT pg_size_pretty(pg_total_relation_size(relid)) FROM pg_stat_user_tables.

2. 3 IAM users with console access have no MFA

Users dev-ops-james, ml-admin-backup, and ci-deploy have AWS Management Console login enabled (confirmed via GetLoginProfile) but have no MFA device registered (ListMFADevices returns empty). All three accounts have been in this state since the initial scan on 1 April 2026.

Impact: A stolen or phished password gives full Console access to the production account with no second factor. dev-ops-james has AdministratorAccess. ml-admin-backup has IAM write permissions. Either account being compromised gives an attacker the ability to create new IAM users, modify security groups, export data from S3, or disable CloudTrail.

Action: Require MFA for console login immediately via an IAM policy with Condition: aws:MultiFactorAuthPresent = false !Deny all actions except iam:CreateVirtualMFADevice and iam:EnableMFADevice. Notify the three affected users and give them 48 hours to enroll before the policy is applied. Consider using IAM Identity Centre to centralise MFA enforcement.

3. No CloudWatch alarms on RDS — blind to performance and storage events

DescribeAlarms returns no alarms targeting ml-prod-pg-primary for any metric. Metrics checked: CPUUtilization, FreeStorageSpace, DatabaseConnections, ReadLatency, WriteLatency. Open since initial scan 1 April 2026.

Impact: There is no automated alerting for the storage issue described above. The team will only discover storage exhaustion, CPU saturation, or connection limit breaches when the application starts failing — not before. The average time-to-detect for database incidents without alarms is typically 15–45 minutes, during which users experience errors.

Action: Create the following alarms targeting ml-prod-pg-primary: (1) FreeStorageSpace < 50,000 MB — threshold 1 period at 5 minutes, SNS alert; (2) CPUUtilization > 80% — threshold 3 periods at 5 minutes; (3) DatabaseConnections > 900 — RDS default max_connections for db.r6g.2xlarge is ~1,000. Route alarms to an existing SNS topic or create a new one targeting the on-call email.

Cost Summary

Estimated 30-day total: $9240.00

Service	30-day Cost
EC2	$4100.00
RDS	$2850.00
Data Transfer	$890.00
CloudFront	$720.00
S3	$430.00
Other	$250.00

Recommendations

[HIGH] 1. Renew ACM certificate immediately
11 days remaining. Enable DNS auto-renewal in ACM to prevent recurrence. Fix in 20 minutes — no downtime required.

[HIGH] 2. Close public internet access to PostgreSQL
Remove 0.0.0.0/0 from sg-0a4f2c1d inbound rules and replace with the application subnet CIDR. Immediate effect, no downtime. Open 24 days with no action taken.

[MEDIUM] 3. Enable RDS storage autoscaling
Storage at 87% and growing ~10 GB/week. Enable autoscaling to maximum 1,000 GB to avoid a read-only failure event in 6–7 weeks.

[MEDIUM] 4. Enforce MFA on three IAM console users
dev-ops-james has AdministratorAccess with no MFA. Apply a Deny policy and notify affected users. Consider migrating to IAM Identity Centre.

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