plainfra

Weekly Health Report

Account: sandbox (471000000001)

Customer: thornwick-logistics-a1b2c3d4 | Report date: 2 Nov 2026

STATUS: AMBER

read-only AWS API

Generated using read-only AWS API access. plainfra inspected infrastructure metadata and configuration only. It did not create, change, or delete infrastructure.

Executive Summary

Sandbox is AMBER with three warnings and no critical findings. CloudTrail is logging again, which closes last week's gap, but two new S3 buckets have no public access block and GuardDuty is still off.

Costs

October 2026 (last full calendar month)

$1,217

Aug $1,187.33 | Sep $1,198.40 | Oct $1,217.06

Service	Oct 2026 cost
Amazon Elastic Compute Cloud - Compute	$763
EC2 - Other	$183
Amazon Simple Storage Service	$115
Amazon Relational Database Service	$90
AWS Lambda	$37
Amazon Virtual Private Cloud	$30

October came to $1,217.06, slightly above September, with no step changes inside the bill window. The t3.large developer instances are almost two thirds of it.

Estate at a Glance

Regions in use: ap-southeast-2

EC2 instances	9	Lambda functions	8
ECS services	0	S3 buckets	17
RDS databases	1	DynamoDB tables	3
Load balancers	0	VPCs	2
Security groups	27	IAM users	8

Security Posture

CloudTrail	**Logging**
MFA	**8 of 8 users**
Password policy	**Default policy**
GuardDuty	**Not enabled**
Security Hub	**Not enabled**
Open security groups	**None open to the internet**
S3 public-access block	**2 buckets without a public-access block**

Scan Coverage

All 29 checks in this scan returned data, so the counts above are exact.

Changed Since Last Report

NEW	S3 buckets without Public Access Block
RESOLVED	CloudTrail logging is on again

Critical Findings

No critical findings.

Warnings

WARNING 1. No password policy with console users

Account password policy uses AWS defaults (no custom policy) and 6 IAM users have console access.

Why it matters: Six people can sign in to the console with passwords that only have to meet the AWS defaults.

Next action: Set an account password policy under IAM account settings: a minimum length of 14 characters and no reuse of recent passwords.

WARNING 2. S3 buckets without Public Access Block

2 of 17 S3 buckets lack a Public Access Block configuration.

Why it matters: Without a public access block, one mistaken bucket policy or ACL is enough to make data public.

Next action: Turn on Block Public Access for the two buckets, or once for the whole account so every bucket, new ones included, is covered.

WARNING 3. GuardDuty is disabled

GuardDuty is not enabled in this account.

Why it matters: Nothing is watching this account for signs of stolen credentials or unusual API activity.

Next action: Enable GuardDuty in ap-southeast-2. Its core detection reads AWS's own logs, so there is nothing to install.

Top 5 Spends

Billed usage from 2 Oct 2026 to 31 Oct 2026, this account only.

#	Spend line	30-day cost	Share
1	**EC2 instance hours (t3.large)** Amazon Elastic Compute Cloud - Compute | ap-southeast-2 Behind it: dev-alice-box, dev-ml-notebook, dev-load-test *The developer instances, including the notebook and load-test machines.*	$738.00	62.7%
2	**EBS gp3 volume storage** EC2 - Other | ap-southeast-2 *Disk volumes attached to the developer instances.*	$106.20	9%
3	**Data stored** Amazon Simple Storage Service | ap-southeast-2 Behind it: thornwick-sandbox-export-trial, thornwick-sandbox-artifacts *Objects stored in the sandbox buckets, including the new export trial bucket.*	$94.35	8%
4	**RDS instance hours (db.t4g.micro)** Amazon Relational Database Service | ap-southeast-2 *A small PostgreSQL scratch database.*	$87.00	7.4%
5	**NAT gateway hours** EC2 - Other | ap-southeast-2 *The NAT gateway that gives the private subnets a way out to the internet.*	$70.80	6%

Notes

Security Hub is disabled
Security Hub is not enabled in this account.

Next Actions

1. Set an account password policy under IAM account settings: a minimum length of 14 characters and no reuse of recent passwords.
2. Turn on Block Public Access for the two buckets, or once for the whole account so every bucket, new ones included, is covered.
3. Enable GuardDuty in ap-southeast-2. Its core detection reads AWS's own logs, so there is nothing to install.

Questions about this report? Contact support@plainfra.com.