AWS Bill Too High? 7-Point Self-Audit

A practical checklist to find hidden waste and risky misconfigurations

Mariusz Gebala — HAIT

2026 EDITION

Most AWS bills grow 20-40% faster than the workload justifies. The causes are rarely obvious — NAT data transfer, forgotten log retention, overprovisioned databases, and duplicated security controls add up silently.

This checklist is what I run through first on every audit. It takes about 20 minutes if you know your account. If something on this list surprises you, there is probably money to reclaim.

Where AWS bills secretly bleed money

1. NAT Gateway data transfer

NAT Gateway charges $0.045/GB processed. A single misconfigured service routing traffic through NAT instead of a VPC endpoint can add $500-2,000/month silently.

Check: Cost Explorer → filter by NAT Gateway → last 30 days.

2. CloudWatch Logs without retention

Default retention is forever. A busy Lambda or ECS cluster can generate 50-200 GB/month of logs nobody reads. At $0.03/GB/month storage, that compounds fast.

Check: List all Log Groups without a retention policy set.

3. Idle EC2 and unattached EBS / EIP

Stopped EC2 instances still pay for EBS. Unattached EBS volumes and Elastic IPs sitting unused cost money every hour. Most accounts have 3-5 of these.

Check: Find instances with <5% average CPU over 14 days.

4. Overprovisioned RDS and ElastiCache

Production database on db.r6g.2xlarge when db.r6g.large would do. RDS right-sizing recommendations exist but most teams never check them.

Check: Review RDS Performance Insights → CPU and memory utilization.

5. Public exposure generating unnecessary traffic

S3 buckets, ALBs, or EC2 instances open to the internet attract scanning bots. The traffic itself costs money through data transfer and WAF charges.

Check: Audit Security Groups with 0.0.0.0/0 inbound rules.

6. Duplicated security controls

Running WAF + AWS Network Firewall + a third-party NGFW on the same traffic path. Each layer has its own cost. Often one or two layers are redundant.

Check: Map which services inspect the same traffic flow.

7. Bad firewall architecture

A GWLB + Palo Alto VM-Series stack can cost $9,287/month for a 3-AZ deployment. Sometimes a simpler architecture with AWS Network Firewall achieves the same security goal for $747/month.

Check: Review the full infrastructure cost stack, not just license fees.

Self-check: verify yourself in 20 minutes

- [ ] Check NAT Gateway data transfer cost in Cost Explorer (last 30 days)
- [ ] List CloudWatch Log Groups without retention policy set
- [ ] Find EC2 instances with <5% average CPU utilization (14 days)
- [ ] Review RDS right-sizing recommendations in Performance Insights
- [ ] Audit Security Groups with 0.0.0.0/0 inbound rules
- [ ] List unattached EBS volumes and unused Elastic IPs
- [ ] Review firewall layers processing the same traffic

Ran the checklist and still have questions?

Book a **free 20-minute video triage** where I walk through your AWS bill with you and point out concrete places to look. No commitment. If I can't find meaningful savings or security issues, I'll tell you straight.

Book at: https://cal.com/haitmg/aws-triage

Or email: kontakt@haitmg.pl

About the author

Mariusz Gebala — Cloud & DevOps Engineer. From 100+ AWS accounts managed (including multi-year engagements with a Fortune 500 networking vendor), I built cloud-audit, an open-source AWS security scanner featured in Help Net Security (March 2026).

Certifications: AWS Solutions Architect Associate · Azure Administrator Associate · Palo Alto PCNSA

Full service page: https://haitmg.pl/aws-cost-security-audit/