

Runbook: AWS WAF Cost Control for CloudFront

Last updated: 2026-01-23

Purpose

Control or eliminate unexpected AWS WAF charges associated with CloudFront distributions.

Symptoms

- AWS Billing shows WAF charges despite low traffic
- CloudFront distribution has a Web ACL associated unintentionally
- You created WAF rules during setup and forgot to detach

Immediate Actions

- Identify Web ACL associated with the CloudFront distribution.
- If not needed, detach the Web ACL from CloudFront.
- Delete unused Web ACLs and rule groups (careful in shared accounts).

Terraform Guidance

- Make Web ACL optional via a variable (enable_waf).
- If enable_waf=false, ensure aws_cloudfront_distribution.web_acl_id is null/omitted.
- Tag Web ACL resources clearly by env (dev/prod) to avoid accidental reuse.

Post-Change Verification

- Confirm CloudFront distribution shows 'Web ACL: None'.
- Monitor billing for 24–48 hours to confirm charges stop.