Engineer Platform

Har bygget fail-closed rate limiting mod misbrug

Har bygget fail-closed misbrugskontroller — 22 Redis-baserede rate limiters, Cloudflare Turnstile, idempotens på requests og en origin-lås — så platformen afviser bots og flood-angreb i stedet for at stole på dem, der kalder den.

2025

22

rate limitere, der lukker ved fejl

Situation. Et offentligt katalog over virksomheder og fagfolk er et mål fra den dag, det går i luften. Scrapere vil have dataene, spamkonti vil have rækkevidden, og et endpoint, der koster platformen rigtige penge at levere — søgning, eksport, alt, der rører et eksternt API — er værd at misbruge alene, fordi det er gratis at kalde. Intet af det er ondskab rettet mod netop denne platform; det er bare hverdagskost på det åbne internet.

Opgave. De dyre stier og dem, der inviterer til misbrug, havde brug for grænser, der holder under pres — også det pres, der opstår, når limiterens egen afhængighed er nede.

Handling. Der er 22 rate limitere, hver bygget til den sti, den beskytter, i stedet for ét globalt loft, fordi et loginforsøg, en søgning og en bulkeksport bliver til misbrug ved vidt forskellige hastigheder. Tilstanden ligger i Redis, så en grænse deles på tværs af instanser og ikke gælder pr. proces, hvor den er let at slippe uden om. Den vigtige beslutning er, hvad der sker, når Redis ikke er der: limiterne er fail-closed. Trafik afvises frem for at blive vinket igennem, hvilket er det mindre bekvemme svar og det eneste forsvarlige. Omkring dem sidder Cloudflare Turnstile på de stier, der er værd at udfordre, 351 linjers idempotency-middleware, så en skrivning, der bliver forsøgt igen, ikke bliver til to, en origin-lås, der afviser requests, som ikke kommer ind ad hoveddøren, og en skræddersyet challenge på selve kataloget.

Resultat. Misbrug bliver dyrt for den, der misbruger, og billigt for platformen, og et udfald i limiterens eget lager ender i afvisning og ikke i en åben dør. At være fail-closed betyder ganske vist, at et Redis-problem bliver et problem, brugeren kan se — det er accepteret med vilje, fordi alternativet er, at et Redis-problem bliver et problem på regningen.

Brug erfaringen i jeres projekt

Brug »Har bygget fail-closed rate limiting mod misbrug« som udgangspunkt for en lignende udfordring i jeres organisation. Ydelserne bag arbejdet kan også bruges i jeres projekt. Overvågning og alarmer, der siger til, mens fejlen stadig er lille, og tallene, der viser, hvor tit den bliver ved med at være det.

Se vores ydelser Kontakt os →

Se bag resultatet

Læs om situationen, beslutningerne og resultatet i eksemplet. Vi kan drøfte, hvad der passer til jeres vilkår, og hvad der kræver en anden tilgang. Har bygget fail-closed rate limiting mod misbrug — 22 rate limitere, der lukker ved fejl

Se vores ydelser Kontakt os →

Bliver du bombarderet af bots og scrapers?

Tal om jeres projekt med den ingeniør, der har ansvaret for leverancen. Vi aftaler omfang, prisgrundlag og overdragelse skriftligt, før arbejdet begynder.

Rolle i opgaven: Sikkerhedsingeniør. Det trækker på Backend-udvikling, API'er & integration, Driftssikkerhed & backup, Netværk & VPN, Sikkerhed og Optimering af ydeevne. Og når I alligevel er her, er vi ret dygtige til Backend- & API-udvikling, Site reliability & overvågning, Sikkerhed & adgangsstyring og Sikkerhed for AI-agenter.

Kontakt os Se vores ydelser

Ét stykke af **en længere fortegnelse** — og det hele ligger her på sitet.

Hver post er skrevet på samme måde: situationen, opgaven, hvad vi gjorde, og hvad der ændrede sig.

Se hele fortegnelsen

Definér den ønskede forbedring

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Bliver du bombarderet af bots og scrapers?

Spørg til beslutningerne bag »Har bygget fail-closed rate limiting mod misbrug«. I taler med mennesker, der kan forklare arbejdet og vurdere jeres eget projekt.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://platform.engineer.company/da/portfolio/built-fail-closed-rate-limiting-and-anti-abuse/