Engineer

Limitation de débit et protection contre les abus

Conçu des protections contre les abus qui refusent l'accès en cas de défaillance — 22 limiteurs de débit Redis, Cloudflare Turnstile, idempotence des requêtes et verrouillage de l'origine — pour rejeter robots et inondations de requêtes sans faire confiance aux appelants.

2025

22

limiteurs de débit qui refusent en cas de défaillance

Situation. Un annuaire public d'entreprises et de professionnels devient une cible dès son ouverture. Les collecteurs veulent les données, les comptes de spam veulent l'audience et une opération coûteuse pour la plateforme — recherche, export ou appel à une API externe — peut être détournée simplement parce qu'elle est gratuite à appeler. Il ne s'agit pas forcément d'une hostilité particulière envers la plateforme, mais de l'environnement ordinaire de l'Internet ouvert.

Tâche. Les chemins coûteux ou détournables avaient besoin de limites résistantes sous pression, y compris lorsque la dépendance du limiteur lui-même devenait indisponible.

Action. 22 limiteurs de débit ont été conçus pour les chemins protégés, plutôt qu'un plafond global unique : une tentative de connexion, une recherche et un export massif deviennent abusifs à des fréquences très différentes. Leur état réside dans Redis pour partager les limites entre instances, au lieu d'avoir des compteurs par processus faciles à contourner. Le choix déterminant concerne l'absence de Redis : les limiteurs refusent l'accès. Le trafic est rejeté plutôt que laissé passer, solution moins commode mais seule défendable. Autour figurent Cloudflare Turnstile sur les chemins nécessitant une

épreuve, 351 lignes de middleware d'idempotence pour éviter qu'une écriture réessayée ne devienne double, un verrou d'origine rejetant les requêtes ne passant pas par l'entrée prévue et une épreuve spécifique pour l'annuaire.

Résultat. L'abus devient coûteux pour son auteur et peu coûteux pour la plateforme. Une panne du stockage des limites produit un refus plutôt qu'une porte ouverte. Ce refus signifie qu'un problème Redis devient visible pour l'utilisateur, compromis accepté pour éviter qu'il ne devienne plutôt un problème de facturation.

Mettez cette expérience au service de votre projet

Prenez « Limitation de débit et protection contre les abus » comme point de départ pour un défi similaire dans votre organisation. Les prestations mobilisées pour cette réalisation sont disponibles pour votre projet. La partie invisible pour les utilisateurs : où résident les données, quelles règles s'appliquent et comment les autres systèmes peuvent y accéder.

Découvrir nos prestations Contactez-nous →

Examinez ce qui a conduit au résultat

Découvrez la situation, les décisions et le résultat de cet exemple. Nous pouvons discuter des éléments transposables à vos contraintes et de ceux qui nécessitent une autre démarche. Limitation de débit et protection contre les abus — 22 limiteurs de débit qui refusent en cas de défaillance

Découvrir nos prestations Contactez-nous →

Robots et collecteurs de données submergent votre service ?

Discutez de votre projet avec l'ingénieure responsable de sa réalisation. Nous convenons par écrit du périmètre, de la base tarifaire et de la transmission avant le début des travaux.

Rôle exercé dans ce contexte : Ingénieure sécurité. Cette réalisation fait appel à Ingénierie backend, API et intégration, Fiabilité et sauvegardes, Réseaux et VPN, Sécurité et Optimisation des performances. Et puisque vous êtes ici, nous sommes aussi plutôt doués en Développement backend et API, Fiabilité des services et supervision, Sécurité et gestion des accès et Sécurité des agents d'IA.

Contactez-nous Découvrir nos prestations

Un élément **d'un parcours plus long** —
entièrement présenté sur ce site.

Chaque entrée suit la même structure : la situation, la tâche, ce que nous avons fait et ce qui a changé.

Voir l'ensemble du parcours

Définissez l'amélioration nécessaire

Présentez le processus de travail, les interfaces existantes et les utilisateurs qui ont besoin du changement. Nous pouvons définir une livraison testable et une transmission permettant à votre équipe d'assurer la maintenance des éléments livrés.

Consulter les tarifs Contactez-nous →

Robots et collecteurs de données submergent votre service ?

Interrogez-nous sur les décisions qui sous-tendent « Limitation de débit et protection contre les abus ». Vous parlerez aux personnes capables d'expliquer le travail et d'évaluer votre propre projet.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

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

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/portfolio/built-fail-closed-rate-limiting-and-anti-abuse/