Engineer

Budget d'erreur

part de défaillances qu'un objectif de fiabilité autorise

Ce que c’est

Un budget d’erreur est la quantité de défaillances qu’un service peut connaître sur une période donnée, calculée à partir de son objectif de niveau de service. Si l’objectif exige la réussite de 99,99 % des requêtes ce trimestre, les 0,01 % restants constituent le budget : des requêtes qui peuvent échouer, par accident ou à la suite d’un risque délibéré, sans que personne ait manqué à une promesse. Il se compte dans la même unité que l’objectif, généralement en requêtes échouées, et se consomme dès que les utilisateurs rencontrent une défaillance.

L’idée vient du livre *Site Reliability Engineering* de Google. Dans le chapitre sur l’acceptation du risque, la gestion de produit fixe l’objectif, la supervision agit comme un tiers neutre qui mesure ce qui s’est réellement produit, et l’écart entre les deux représente la marge de défaillance encore disponible pour le trimestre. Développement produit et SRE conviennent ensemble de ce budget à l’avance. L’exemple du livre se situe dans le haut de l’échelle d’exigence : un service devant répondre à 99,999 % des requêtes dispose d’un budget de 0,001 %. Un seul problème faisant échouer 0,0002 % des requêtes du trimestre en consomme donc un cinquième.

Le budget ne demande pas à qui la défaillance est imputable. Le livre précise qu’une panne réseau ou la défaillance d’un centre de données le consomme exactement comme une mauvaise mise à disposition, et que le reste du trimestre peut dès lors comporter moins de livraisons. Les utilisateurs ont subi la défaillance ; elle compte donc. Savoir qui doit agir est une autre question, dont la réponse doit figurer dans une politique écrite et convenue avant le premier problème.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un budget d'erreur ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Une supervision et des alertes qui signalent les incidents tant qu'ils restent mineurs, avec les chiffres qui montrent à quelle fréquence ils le restent.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. Premier tableau de bord d'observabilité — première vue de l'entreprise sur ses propres systèmes

Premier tableau de bord d'observabilité Contactez-nous →

Pourquoi c’est important

Les personnes qui livrent des fonctionnalités et celles qui maintiennent un service en fonctionnement n’ont pas les mêmes objectifs. Sans chiffre partagé, leur débat est remporté par la partie qui négocie le mieux. Le livre SRE estime que ces décisions ne devraient reposer ni sur la politique, ni sur la peur, ni sur l’espoir, et rappelle la devise officieuse des SRE de Google : « L’espoir n’est pas une stratégie. » Le budget remplace le débat par un chiffre accepté au préalable par les deux parties. Tant qu’il reste du budget, les mises à disposition se poursuivent. Lorsqu’il est épuisé, elles s’arrêtent et l’effort se porte sur les tests et la résilience. Le livre décrit aussi des variantes plus progressives de cette boucle : ralentir les mises à disposition ou revenir en arrière à l’approche de l’épuisement. Une note appelle la version binaire une commande tout ou rien, ou bang/bang control.

L’effet le plus intéressant porte sur les comportements. Quand le budget est large, les développeurs peuvent prendre des risques : livrer plus souvent, tenter l’expérience. Quand il est presque épuisé, observe le livre, les développeurs demandent eux-mêmes plus de tests et des livraisons plus lentes, car personne ne veut bloquer son propre lancement. L’équipe se régule d’elle-même. Le livre pose une condition : cela ne fonctionne que si les SRE ont réellement l’autorité d’arrêter les lancements une fois l’objectif enfreint.

Le budget gouverne principalement les mises à disposition parce que ce sont surtout elles qui provoquent les pannes : l’exemple de politique du *SRE Workbook* attribue environ 70 % des interruptions de Google aux changements. Le budget indique donc où porter l’effort. Le chapitre du Workbook sur la mise en œuvre des SLO étudie un service avec un objectif de 97 % et un budget sur quatre semaines de 109 897 requêtes échouées. Une mauvaise version d’API faisant échouer toutes les requêtes pendant quatre heures en coûte 14 066, soit environ 13 %. Un serveur de base de données qui tombe en panne et demande

20 heures de restauration depuis une sauvegarde en coûte environ 72 000, soit 65 %. La panne du serveur paraît bien pire. Mais l'entreprise de l'exemple n'en subit qu'une en cinq ans, contre deux ou trois mauvaises mises à disposition par an : en moyenne, ces dernières coûtent donc environ deux fois plus de budget. Corriger d'abord le processus de mise à disposition est plus rentable.

Un budget qui n'est jamais consommé dit aussi quelque chose. Le livre note qu'il révèle le coût d'un objectif excessivement élevé en rigidité et en lenteur d'innovation. Une équipe qui peine à lancer peut choisir d'assouplir son objectif, ce qui agrandit le budget.

À quoi cela ressemble en pratique

La consommation a une vitesse aussi bien qu'un total. Le chapitre du Workbook sur les alertes appelle cette vitesse le taux de consommation, ou burn rate : la rapidité avec laquelle le service consomme son budget, relativement à l'objectif. À un taux de 1, le budget s'épuise exactement à la fin de la fenêtre. Pour un objectif de 99,9 % sur 30 jours, son tableau donne ceci :

Taux de consommation	Taux d'erreur	Budget épuisé après
1	0,1 %	30 jours
2	0,2 %	15 jours
10	1 %	3 jours
1 000	100 %	43 minutes

Alerter sur le taux de consommation vaut mieux que déclencher une alerte d'astreinte dès que les erreurs dépassent 0,1 %, ce qui réveillerait quelqu'un à chaque pointe brève. Le Workbook recommande de surveiller plusieurs taux à la fois, chacun sur une fenêtre longue et une courte. Son point de départ pour un objectif de 99,9 % déclenche une alerte d'astreinte lorsque 2 % du budget de 30 jours est consommé en une heure, soit un taux de 14,4, ou 5 % en six heures, soit un taux de 6. Il ouvre un ticket lorsque 10 % est consommé en trois jours, soit un taux de 1. La fenêtre courte, égale au douzième de la longue, permet à l'alerte de s'arrêter peu après le problème. Dans l'exemple du Workbook, les erreurs cessent et, cinq minutes plus tard, la moyenne sur la fenêtre courte repasse sous le seuil, tandis que la moyenne sur une heure reste au-dessus pendant une heure entière.

Dans un fichier de règles Prometheus, les deux conditions d'alerte d'astreinte s'écrivent ainsi. Les ratios sont des règles d'enregistrement nommées comme dans le Workbook ; chacune contient la part des requêtes échouées sur la fenêtre indiquée dans son nom :

```
groups:
  - name: orders-error-budget
    rules:
      - alert: OrdersErrorBudgetBurn
        expr: |
          (
            job:slo_errors_per_request:ratio_rate1h{job="orders"}
              > (14.4 * 0.001)
            and
            job:slo_errors_per_request:ratio_rate5m{job="orders"}
              > (14.4 * 0.001)
          )
          or
          (
            job:slo_errors_per_request:ratio_rate6h{job="orders"}
              > (6 * 0.001)
            and
            job:slo_errors_per_request:ratio_rate30m{job="orders"}
              > (6 * 0.001)
          )
        labels:
          severity: page
```

Suivons un mauvais déploiement à travers ces règles. À 14:00, une mise à disposition commence à faire échouer 2 % des requêtes liées aux commandes, soit un taux de consommation de 20. Le ratio sur cinq minutes dépasse le seuil de 1,44 % en quatre minutes au plus. Celui sur une heure ne l'atteint toutefois qu'après environ 43 minutes d'erreurs ; l'alerte d'astreinte part donc vers 14:43. À ce moment, exactement 2 % du budget mensuel est consommé. C'est le compromis de la règle : un bref incident ne réveille personne et une consommation soutenue ne peut pas se cacher. Rétablissez la version précédente à 14:50 : le ratio sur cinq minutes repasse sous le seuil en deux minutes au plus et met fin à l'alerte. Le seul ratio sur une heure l'aurait maintenue jusqu'à environ 15:07.

Maintenir des alertes d'astreinte proportionnées est aussi l'idée derrière la supervision des erreurs et le traçage développés en propre pour la plateforme de l'entreprise, travail réalisé dans le cadre d'un poste occupé depuis 2025. Cette solution détecte les pointes et les régressions avec une temporisation qui limite

la répétition des alertes pour qu'un mauvais déploiement ne déclenche pas quarante alertes d'astreinte. Ses règles d'alerte ont été adaptées à cette plateforme plutôt qu'à un cas générique, et l'une de ses 11 vues destinées aux opérateurs est consacrée aux objectifs de niveau de service.

Où les problèmes surviennent

Le décompte des défaillances se confond avec la recherche d'un responsable. Tout ce que les utilisateurs subissent consomme le budget, mais tout ne devrait pas arrêter les mises à disposition de l'équipe elle-même. L'exemple de politique du Workbook permet de poursuivre le développement de fonctionnalités lorsqu'un problème réseau touchant l'entreprise entière a causé l'interruption, ou lorsqu'un service d'une autre équipe l'a provoquée et que cette équipe a gelé ses mises à disposition. Quand un bug ou une procédure de l'équipe elle-même a consommé le budget, la fiabilité passe en premier. Pour une interruption due à une dépendance gérée par une autre équipe, le chapitre sur la mise en œuvre des SLO présente deux approches : continuer ou geler malgré tout. Il estime que le gel satisfait davantage les utilisateurs. Choisissez à l'avance, écrivez ce choix dans la politique et désignez qui tranche un désaccord sur le calcul ; l'exemple de politique confie cette décision au CTO.

Les erreurs sont classées dans la mauvaise catégorie. Un test de charge en échec ou les requêtes rejetées d'un testeur d'intrusion consomment du budget alors qu'aucun utilisateur n'a été touché. L'exemple de politique cite les erreurs mal classées comme une façon de perdre du budget pour rien. L'inverse est pire : de véritables défaillances classées comme anodines maintiennent sur le papier le service dans son objectif alors que les utilisateurs souffrent. La même politique rend le travail de fiabilité obligatoire quand cette situation est découverte. Excluez de l'indicateur le trafic que l'objectif ne couvre pas et vérifiez le classement après tout incident dont le coût paraissait erroné.

Un incident majeur consomme du budget, puis est oublié. Un gel fait gagner du temps sans pour autant expliquer ce qui s'est passé. L'exemple de politique lie les deux : un seul incident consommant plus de 20 % du budget de quatre semaines exige une analyse après incident avec au moins une action de la plus haute priorité. Une catégorie d'interruptions consommant plus de 20 % en un trimestre doit figurer au programme du trimestre suivant.

L'alerte ne peut jamais se déclencher. Des seuils copiés du tableau à 99,9 % ne se transposent pas à d'autres objectifs. À 90 % de disponibilité, souligne le Workbook, une interruption totale ne consomme que 1,4 % du budget en une heure. Une règle déclenchant l'astreinte à 2 % par heure reste donc silencieuse pendant toute l'interruption. À l'autre extrême, un objectif mensuel de 99,999 % s'épuise en 26 secondes d'interruption totale, avant même que de nombreux systèmes de supervision aient recueilli un échantillon. Adaptez les fenêtres et les seuils à l'objectif. Pour les objectifs très élevés, acceptez la conclusion du Workbook : seule la conception du système peut permettre de les respecter. Déployez d'abord un changement auprès de 1 % des utilisateurs, et la même défaillance laisse 43 minutes avant l'épuisement du budget.

Un faible trafic transforme une seule défaillance en alerte d'astreinte. À dix requêtes par heure, une requête échouée représente un taux d'erreur de 10 % sur l'heure. Pour un objectif de 99,9 %, note le Workbook, cette requête déclenche immédiatement l'astreinte parce qu'elle consomme 13,9 % du budget de 30 jours : le mois entier n'autorise que sept échecs. Le Workbook propose de générer du trafic artificiel, de regrouper plusieurs petits services pour la supervision ou de modifier le produit afin qu'une seule requête échouée ait moins d'importance.

L'objectif est relevé avant que le service puisse l'atteindre. Une équipe qui a besoin d'un objectif plus exigeant et l'adopte immédiatement vit dans l'urgence permanente, avec un budget toujours épuisé. Le Workbook propose plutôt un objectif à viser : mesuré et suivi à côté de l'actuel, mais désigné dans la politique comme n'exigeant aucune action tant que le service n'est pas prêt à l'atteindre.

Pour aller plus loin

- Accepter le risque — le chapitre 3 du livre *Site Reliability Engineering* de Google, qui présente le budget d'erreur comme moyen de décider des mises à disposition à partir de données.
- Alertes sur les SLO — le *SRE Workbook* sur les taux de consommation, les alertes à plusieurs fenêtres et les services à faible trafic.
- Exemple de politique de budget d'erreur — une politique complète : arrêt des mises à disposition, interruptions exemptées et cas exigeant une analyse après incident.
- Mettre en œuvre les SLO — calculer un budget à partir d'un objectif et l'employer pour choisir les investissements de fiabilité.
- Règles d'alerte — la documentation Prometheus du format de fichier de règles utilisé ci-dessus.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un budget d'erreur ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

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/glossary/error-budget/