Engineer Plateforme

Fiabilité et sauvegardes

43 réalisations

Reliez les parties de votre système

Les réalisations regroupées sous « Fiabilité et sauvegardes » montrent une partie d'un système opérationnel. Nous pouvons vous aider à relier cette partie au reste de votre activité. 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 →

Trouvez un défi comparable

Suivez un exemple qui ressemble à votre situation. Son analyse décrit les décisions qui ont conduit au résultat, au-delà du nom de la technologie. Premier tableau de bord d'observabilité — première vue de l'entreprise sur ses propres systèmes

Premier tableau de bord d'observabilité Contactez-nous →

Premier tableau de bord d'observabilité

Développé et lancé le premier tableau de bord d'observabilité de l'entreprise, affichant en temps réel les performances du système et des visualisations de données sur le grand téléviseur des bureaux.

10 serveurs PostgreSQL et MS SQL sur Ubuntu

Conçu, déployé et maintenu 10 serveurs PostgreSQL et MS SQL sur des VPS Ubuntu Linux, en veillant à leurs performances et à leur fiabilité.

Déploiement SaaS GIS automatisé : GitHub Actions

Automatisé le déploiement d'une application SaaS GIS, le traitement des données et le système de reporting avec GitHub Actions CI/CD, Python, Bash et SQL.

Livraison de 20 pipelines GIS automatisée

Automatisé la livraison de 20 pipelines de données GIS et processus ETL de données applicatives, en simplifiant l'automatisation de l'infrastructure et le reporting.

100 sauvegardes critiques automatisées : Barman

Automatisé 100 sauvegardes critiques avec Barman, Google Cloud, Bash et Python pour préserver l'intégrité des données dans les bases.

20 applications Docker sur Google Cloud et AWS

Déployé et maintenu 20 applications conteneurisées avec Docker, résolu des incidents avec Podman et Kubernetes et géré des applications R sur Google Cloud et AWS.

30 instances VPS Ubuntu Linux administrées

Géré 30 instances VPS Ubuntu Linux, mis en place des stratégies de reprise après sinistre et adapté les configurations réseau.

Risques réduits avec Grafana et Prometheus

Réduit les risques d'exploitation en mettant en place un tableau de bord de supervision avec Grafana et Prometheus pour améliorer la fiabilité du système.

8 connexions VPN WireGuard et IPsec gérées

Géré et dépanné 8 connexions VPN WireGuard et IPsec, en sécurisant les communications entre Google Cloud et les systèmes Linux.

Infrastructure réseau administrée

Administré l'infrastructure réseau de plus de 1 000 serveurs, en veillant à leur déploiement, à leur sécurité et à la résolution des incidents.

SSL/TLS automatisé pour 100 applications Docker

Automatisé la création de certificats SSL/TLS pour 100 applications Docker afin de sécuriser les connexions sur des hôtes Ubuntu Linux.

CI/CD simplifiée : 4 000 heures gagnées

Simplifié les processus CI/CD et économisé 4 000 heures grâce à l'automatisation des pipelines de développement logiciel.

1 000 routeurs Wi-Fi configurés et déployés

Configuré et déployé 1 000 routeurs Wi-Fi pour améliorer l'accès au réseau et ses performances pour les clients.

100 serveurs Bare Bone administrés

Administré 100 serveurs Bare Bone, des réseaux physiques et des systèmes de téléphonie IP pour soutenir la croissance de l'entreprise.

40 sites administrés sur Apache et Nginx

Administré 40 sites web sur des serveurs d'hébergement Ubuntu Linux avec Apache et Nginx, en veillant à leur disponibilité et à leurs performances.

Un produit cartographique pris en charge de bout en bout

Conçu l'architecture, développé et maintenu l'infrastructure, le traitement des données et une application cartographique pendant 2 ans, en couvrant la livraison logicielle et la maintenance d'exploitation.

Contrat d'API généré à partir de la base

Généré le contrat d'API à partir de la base de données — OpenAPI, client TypeScript typé de 44 076 lignes, 61 gestionnaires de simulation et limites appliquées par l'interface — avec un contrôle à chaque étape qui échoue en cas de divergence.

E-mails avec basculement et journal de livraison

Conçu l'envoi d'e-mails comme une capacité de plateforme — trois fournisseurs avec basculement, webhooks de livraison, journaux d'envoi et de livraison, modèles et campagnes — avec un contrôle au démarrage qui refuse de lancer le service sans fournisseur.

Infrastructure Azure sous forme de code

Provisionné l'infrastructure Azure sous forme de code avec Bicep — Container Apps, PostgreSQL Flexible Server, Front Door/WAF et réseau — dans les environnements de développement, de préproduction et de production.

Pipelines CI/CD GitHub Actions

Conçu des pipelines GitHub Actions CI/CD avec une image frontend de production distroless et une promotion entre plusieurs environnements.

Déploiements Azure pris en charge de bout en bout

Pris en charge les déploiements de bout en bout sur Azure, en gérant les livraisons dans les environnements de développement, de préproduction et de production.

Sauvegardes et reprise sous forme de code

Configuré la conservation des sauvegardes sous forme d'Infrastructure as Code, puis évalué les possibilités de récupération et documenté la restauration, en explicitant les lacunes restantes avant qu'un incident ne les révèle.

Assistance 24/7 : environ 1 000 serveurs IPTV/OTT

Assuré une assistance infrastructure 24/7 pour une plateforme de diffusion IPTV/OTT, en administrant environ 1 000 serveurs et des systèmes appartenant aux clients pour une clientèle mondiale en Chine, aux États-Unis et en Allemagne.

Continuité des flux de diffusion IPTV

Assuré la continuité de l'acheminement des flux IPTV entre fournisseurs et clients, en supervisant et maintenant le réseau de diffusion et la téléphonie IP jour et nuit.

Infrastructure durable, encore en service

Planifié et mis en œuvre de nouvelles fonctionnalités d'infrastructure pour des systèmes internes et externes, avec des solutions assez durables pour fonctionner encore des années plus tard avec peu de changements.

Suite de tests Go, SQL et navigateur

Conçu une suite de tests automatisés en couches — 981 tests Go, 543 spécifications frontend et navigateur, 494 tests de comportement SQL — avec tests par mutation, tests fondés sur les propriétés et contrôle obligatoire de l'accessibilité.

Traitements lents confiés à une file River

Sorti les traitements lents du chemin des requêtes pour les confier à une file de tâches River — 15 modules de traitement, 8 tâches planifiées et 20 tâches pg_cron — afin de répondre aux requêtes pendant la poursuite du travail en arrière-plan.

Surveillance des erreurs et traçage internes

Conçu en interne la surveillance des erreurs et le traçage OpenTelemetry plutôt que de les acheter — assainissement des charges utiles, détection des pics et régressions, symbolication et signal de vie synthétique — accessibles dans 11 vues d'exploitation.

1 022 migrations contrôlées contre les écarts

Maintenu la cohérence du schéma au fil de 1 022 migrations avec un contrôle CI construisant la base de deux façons — installation neuve, puis installation suivie de toutes les migrations — et échouant en cas de différence.

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.

Programme continu d'analyse de sécurité

Mis en place un programme continu de sécurité — analyse du code, DAST, contrôles des dépendances et des vulnérabilités, génération de SBOM, détection de secrets et actions épinglées par SHA — accompagné de 21 audits de sécurité écrits.

Une infrastructure définie dans un dépôt

Conçu l'infrastructure de l'entreprise avec 19 playbooks Ansible et 34 rôles totalisant 12 065 lignes de YAML, pour faire converger un hôte en service vers un état déclaré, chaque play étant idempotent.

Services publics sur un petit serveur

Hébergé les services publics de l'entreprise sur un hôte monocœur de 512 MB — forge git, serveur web pour sept domaines, Tor, deux serveurs de protocoles alternatifs et blocage des intrusions — avec 464 MB de mémoire utilisable comme contrainte de conception ; l'automatisation des sauvegardes constitue une mise en œuvre distincte.

Bannissement testé à chaque exécution

Vérifié de bout en bout le blocage des intrusions à chaque exécution du durcissement, en bannissant une adresse réservée aux tests, en lisant la règle noyau obtenue et en levant le bannissement dans un bloc de nettoyage garanti, pour qu'une protection défaillante fasse échouer l'exécution au lieu de se déclarer saine.

Sauvegardes automatisées et méthode de restauration explicite

Mis en place l'automatisation des sauvegardes restic avec conservation, contrôles d'intégrité et procédure mensuelle de test de restauration ; documenté l'activation du stockage et la vérification d'une restauration réelle comme des étapes d'exploitation distinctes.

Supervision par absence de signal de vie

Conçu une supervision par absence de signal de vie qui n'émet un signal que si mémoire et disque sont sains, pour qu'un hôte dégradé déclenche une alerte en se taisant, et corrigé six noms de variables indiquant « free » alors que le contrôle mesurait bien « available », des valeurs d'un ordre de grandeur différent sur une machine de 464 MB.

Mode de vérification Ansible fiabilisé

Fiabilisé le mode de vérification sur toute la plateforme après avoir trouvé six sondes prenant des décisions sur une valeur que l'hôte n'avait jamais fournie : le module command d'Ansible annonce une réussite sous --check tout en sautant entièrement la commande.

Vérification des secrets en une seconde

Ajouté un play de vérification préalable exécutant en une seconde environ le même code que la convergence, avec les secrets locaux de l'opérateur, après qu'une exécution de production partiellement appliquée s'est arrêtée à la neuvième tâche, les paramètres de swap étant déjà écrits sur l'hôte en service.

Secrets d'exploitation séparés par hôte

Séparé les quatre secrets d'exploitation par hôte après avoir établi que deux hôtes partageant un seul signal de vie produisent moins d'alertes que deux signaux distincts, et qu'une phrase secrète de sauvegarde commune peut exposer les sauvegardes des deux hôtes, même dans des dépôts distincts, si une personne l'obtient et peut lire les données chiffrées et les fichiers de clés des deux dépôts.

981 tests et 92 % de couverture

Vérifié le générateur avec 981 cas de test et un seuil de couverture des branches de 92 %, en traitant les avertissements comme des échecs, et vérifié l'idempotence en exécutant deux fois tout le pipeline depuis un fichier vide, sans changement autorisé au second passage.

Un pipeline d'événements borné pour une application macOS

Borné les tampons d'événements et la journalisation après un incident macOS enregistré : croissance de 41 MB par seconde et 111 GB de pages compressées sur une machine de 36 GB ; une exécution complète des tests consignée a réduit les journaux du cœur de 610 996 à 1 411 lignes.

Moitié jusque-là inutilisée du cœur exploitée

Exploité la moitié du cœur de messagerie jusque-là inutilisée — transfert des sauvegardes, messages éphémères, modification et renvoi de messages, invitations vérifiées, proxys et politique de chiffrement — en exécutant chaque test contre la vraie bibliothèque, sans simulations.

Six collecteurs indiquent les entrées ignorées

Fait expliciter à six collecteurs de reporting la partie de leurs entrées jamais lue — fichiers non ouverts, sondes non installées, lignes du journal non reconnues — et ajusté les seuils sur 116 échantillons mesurés, après avoir établi qu'une collecte aveugle et un hôte sain produisaient la même page.

Ciblez l'effort d'ingénierie

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 →

Replacez le sujet dans votre contexte

Dites-nous comment « Fiabilité et sauvegardes » se manifeste dans votre propre système. Nous pouvons vous aider à choisir la prestation pertinente et à définir les travaux correspondants.

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://platform.engineer.company/fr/categories/reliability/