Engineer Plateforme

{ Infrastructure as Code }

Des serveurs que vous pouvez reconstruire à partir d'une configuration versionnée

Toute la configuration décrite dans des fichiers, pour la recréer à l'identique sans qu'elle ne dépende de la mémoire d'une seule personne.

Vous cherchez encore à préciser vos besoins ?

Dites-nous ce qui ne fonctionne pas ou ce que vous essayez de construire. Nous vous dirons ce que cela demanderait, son coût approximatif et si nous sommes les bonnes personnes pour le réaliser.

À partir de 1 400 DKK de l'heure, hors TVA — et un tarif horaire réduit pour une réservation plus longue.

Contactez-nous Consulter les tarifs

Une sélection de réalisations illustrant cette prestation.

Transformez la prestation en résultat

Mettez « Infrastructure as Code » au service d'un résultat pour votre entreprise. Nous pouvons relier le travail technique aux utilisateurs, aux opérations et aux décisions qu'il doit soutenir. Toute la configuration décrite dans des fichiers, pour la recréer à l'identique sans qu'elle ne dépende de la mémoire d'une seule personne.

Contactez-nous

Examinez les réalisations pertinentes

Consultez les réalisations liées sur cette page pour examiner notre démarche. Interrogez-nous sur les compromis et les conditions qui ont conduit à chaque résultat. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

1 000 règles RBAC pour sécuriser Linux

Renforcé la sécurité des données en mettant en place 1 000 règles RBAC pour les développeurs, les instances applicatives, PostgreSQL, MS SQL et d'autres serveurs Linux afin de prévenir les accès non autorisés, avec une documentation et une automatisation Ansible.

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.

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.

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.

SSH durci avec 24 directives validées

Durci SSH avec 24 directives vérifiées et une validation en trois étapes — fichier candidat, configuration assemblée, puis relecture par le démon — après que cette dernière a révélé que le serveur en service remplaçait silencieusement deux des vingt-quatre directives.

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.

Zone DNS de 20 enregistrements en code

Réconcilié déclarativement une zone DNS de 20 enregistrements avec l'API Cloudflare, avec des points d'entrée distincts pour l'audit et l'export BIND, puis désactivé le proxy CDN après sa mise en place pour des raisons de confidentialité.

Exposition des bacs à sable systemd réduite

Réduit l'exposition des bacs à sable systemd de chaque unité installée par la plateforme — service de signal de vie de 9,6 UNSAFE à 1,5, forge git exposée à Internet de 8,3 EXPOSED à 1,5 — et ajouté un contrôle du parseur lors de la convergence après avoir découvert une directive mal orthographiée silencieusement ignorée dans trois modèles d'unités.

Votre code sur votre propre serveur

Déployé la forge git de l'entreprise avec Soft Serve, privée par défaut, sans interface web et avec un port SSH lié à l'interface de bouclage derrière un hôte relais, puis fait de sa page d'accueil un artefact de compilation du site principal plutôt qu'une copie maintenue à la main.

Second serveur provisionné à partir du code

Automatisé le provisionnement d'un second serveur chez un second fournisseur cloud, en créant le pare-feu avant la machine pour qu'elle soit protégée dès sa création, et configuré les pare-feu des deux fournisseurs directement par leurs API REST pour éviter une collection tierce.

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.

Hook CI de forge répété : 2 défauts détectés

Répété l'exécution du hook CI côté forge et trouvé deux défauts impossibles à atteindre par la seule lecture : un mécanisme de repli fournissant un argument impossible à résoudre à l'entrée du hook et une variable d'environnement git suivant le contrôle dans le checkout, faisant échouer 19 tests.

Miroir Tor onion à une adresse lisible

Publié un miroir Tor onion du site à une adresse lisible commençant par engineer, avec une clé générée hors de l'hôte et jamais présente dans ce dépôt ni sur un portable, en conservant ce quatrième point d'entrée comme le seul des quatre à ne jamais être compté.

Vous recherchez une prestation en Infrastructure as Code ?

Consultez les réalisations liées pour évaluer l'expérience pertinente. Dites-nous ce que vous devez construire ; nous pourrons discuter du périmètre, de la démarche de réalisation et de la transmission.

Contactez-nous Portfolio complet

Définissez le périmètre avant de commander les travaux

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 →

Précisez vos besoins avec nous

Dites-nous ce que vous attendez de « Infrastructure as Code », y compris l'échéance et l'équipe qui en assurera la maintenance. Nous pouvons discuter d'une façon concrète d'avancer.

Contactez-nous

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/services/infrastructure-as-code/