Engineer

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.

septembre 2026

chaque unité isolée et une faute jusque-là ignorée

Situation. Treize fichiers d'unité étaient installés par ce dépôt et exécutés sur l'hôte de production avec les privilèges que le superviseur accorde sans configuration particulière, soit la plupart d'entre eux. Un score de durcissement attribuait 9,6 au service d'alarme par absence de signal et le déclarait dangereux ; la forge git exposée à Internet obtenait 8,3 et était déclarée exposée. Les deux chiffres étaient exacts et aucun n'avait déclenché d'action, car un score sans seuil associé est un nombre que l'on apprend à ignorer.

Tâche. Chaque unité avait besoin d'un bac à sable proportionné à ce qu'elle fait réellement, et ces bacs à sable avaient besoin d'un contrôle, car le mode de défaillance d'un bac à sable incorrect est que l'unité démarre puis se casse à un endroit que l'analyseur ne peut pas voir.

Action. Des restrictions de privilèges ont été ajoutées à chaque modèle d'unité — un plafond de privilèges fixé à ceux de l'unité elle-même, un filtre d'appels système, des familles d'adresses restreintes et une mémoire accessible en écriture ou exécutable, mais jamais les deux. Résultats mesurés : le dispositif d'alarme est passé de 9,6 à 1,5, la forge de 8,3 à 1,5, et les deux unités de sauvegarde de 9,6 à 2,3 et 2,5. Leur écriture a révélé mieux que les scores. Une directive était mal orthographiée dans trois modèles d'unité depuis la création de ces rôles — un nom plausible qui n'existe pas, auquel le superviseur répond en journalisant qu'il ne reconnaît pas la clé et en démarrant quand même l'unité. Rechercher une directive prouve qu'elle a été écrite ; seul l'analyseur prouve

qu'elle a pris effet. Un rôle de vérification soumet donc désormais chaque unité au vérificateur du superviseur lui-même pendant la convergence, et est inclus par chaque rôle qui installe une unité. Ce que cela ne peut toujours pas voir est clairement énoncé dans les mêmes documents : chaque directive capable de casser ces unités les casse à l'exécution, pas à l'analyse, et un score ne peut pas dire si un script atteint encore sa dernière ligne.

Résultat. Chaque unité s'exécute avec les privilèges dont elle a besoin et sans ceux dont elle n'a pas besoin, les chiffres sont mesurés plutôt qu'affirmés, et la catégorie de défaut où une faute de frappe devient un contrôle silencieusement absent fait désormais échouer une exécution. Les limites de la mesure sont consignées à côté, ce qui empêche le lecteur suivant de trop se fier à une bande verte.

Mettez cette expérience au service de votre projet

Prenez « Exposition des bacs à sable systemd réduite » comme point de départ pour un défi similaire dans votre organisation. Les prestations mobilisées pour cette réalisation sont disponibles pour votre projet. 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.

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. Exposition des bacs à sable systemd réduite — chaque unité isolée et une faute jusque-là ignorée

Découvrir nos prestations Contactez-nous →

Vos services ont-ils plus d'accès que nécessaire ?

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 fiabilité des services. Cette réalisation fait appel à Infrastructure, Conteneurs (Docker/Kubernetes), Automatisation et CI/CD, Linux et serveurs, Sécurité et Tests et assurance qualité. Et puisque vous êtes ici, nous sommes aussi plutôt doués en Infrastructure as Code, Conteneurisation et orchestration, Administration système et Sécurité et gestion des accès.

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 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 →

Vos services ont-ils plus d'accès que nécessaire ?

Interrogez-nous sur les décisions qui sous-tendent « Exposition des bacs à sable systemd réduite ». 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/cut-systemd-sandbox-exposure-on-every-unit/