Engineer Plateforme

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.

2022 – 2024

1,000

règles d'accès écrites pour
combler une faille de sécurité

Situation. L'organisation devait renforcer les contrôles d'accès dans plusieurs systèmes, notamment les environnements de développement, les instances applicatives, PostgreSQL, MS SQL et les serveurs Linux. Si le modèle RBAC sous-jacent était simple, la difficulté consistait à gérer plus de 1 000 règles individuelles pour couvrir la diversité des rôles utilisateurs et des exigences des systèmes. L'objectif était d'imposer des restrictions d'accès strictes sans introduire de complexité.

Tâche. Mettre en œuvre une solution RBAC évolutive en définissant et en appliquant 1 000+ règles de contrôle d'accès. Cela impliquait d'associer les autorisations à des rôles précis, par exemple les développeurs, les instances applicatives et les administrateurs de bases de données, et de veiller à l'application cohérente des règles dans tous les systèmes. La mission exigeait également de documenter les règles et d'automatiser leur déploiement pour éviter les erreurs manuelles.

Action. L'approche a consisté à créer une structure RBAC simple et modulaire, en répartissant les autorisations en catégories claires et réutilisables, par exemple « accès en lecture seule aux bases de données de production ». Ansible a permis d'automatiser la configuration de chaque règle et de maintenir la cohérence entre les environnements. Par exemple, les développeurs n'avaient accès qu'aux serveurs qui leur étaient attribués, tandis

que les instances applicatives disposaient d'autorisations limitées pour empêcher les déplacements latéraux. Le processus privilégiait la clarté à la complexité, chaque règle étant explicitement liée à un rôle et à un système précis.

Résultat. Le travail consigné couvre 1 000 règles d'accès pour les environnements de développement, les instances applicatives, les bases de données et les serveurs Linux, avec une configuration Ansible documentée. Le résultat livré est un ensemble de règles par rôle et une méthode reproductible pour les appliquer et les examiner. Le dossier ne quantifie ni la réduction du risque de sécurité ni le gain de temps de déploiement.

Mettez cette expérience au service de votre projet

Prenez « 1 000 règles RBAC pour sécuriser Linux » 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. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

Découvrir nos prestations Contactez-nous →

Des accès à mieux contrôler dans vos systèmes ?

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 bases de données. Cette réalisation fait appel à Bases de données, DevOps, Infrastructure, Automatisation et CI/CD, Linux et serveurs, Sécurité, Administration système et Documentation. Et puisque vous êtes ici, nous sommes aussi plutôt doués en Administration de bases de données (DBA), Infrastructure as Code, Administration système, 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 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 →

Des accès à mieux contrôler dans vos systèmes ?

Interrogez-nous sur les décisions qui sous-tendent « 1 000 règles RBAC pour sécuriser Linux ». 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://platform.engineer.company/fr/portfolio/wrote-1000-rbac-rules-to-secure-linux-servers/