La gestion des identités IAM dans le Cloud

Architecture sécurité · https://nuabee.fr/documents/gestion-identites-iam-cloud/

Introduction

La gestion des identités et des accès (IAM) est un composant fondamental des systèmes de sécurité dans le Cloud. Elle permet de contrôler qui peut accéder à quelles ressources dans le Cloud et de quelles manières.

En utilisant IAM, nous avons la capacité de créer des utilisateurs avec des permissions finement ajustées, assurant ainsi que chaque individu n'ait accès qu'aux ressources nécessaires pour accomplir ses tâches. Cette approche minimise les risques liés aux accès non autorisés et renforce la sécurité globale des environnements Cloud de T Cloud Public (anciennement Open Telekom Cloud).

Comprendre la gestion des identités et des accès (IAM) du Cloud

Le composant IAM du Cloud est conçu pour offrir un contrôle granulaire sur les accès aux ressources Cloud. Il permet aux administrateurs de créer et de gérer des utilisateurs, des groupes et des rôles, en définissant des politiques d'accès spécifiques pour chaque entité. Voici les éléments clés :

1. **Utilisateurs et Groupes** : Les utilisateurs sont des entités individuelles qui peuvent se voir attribuer des permissions. Les groupes permettent de regrouper des utilisateurs ayant des besoins d'accès similaires, facilitant ainsi la gestion des permissions à l'échelle.
2. **Rôles et Politiques** : Les rôles sont des ensembles de permissions prédéfinies qui peuvent être attribuées aux utilisateurs ou aux groupes. Les politiques, quant à elles, définissent les permissions spécifiques d'accès et les conditions d'utilisation pour les ressources. Cela permet de contrôler finement qui peut faire quoi, sur quelles ressources et dans quelles conditions.
3. **Permissions** : IAM permet de définir des permissions spécifiques pour des actions précises, telles que la lecture, l'écriture, la modification et la suppression de ressources particulières.

Cela est essentiel pour appliquer le principe du moindre privilège, garantissant que les utilisateurs n'ont accès qu'aux ressources dont ils ont besoin pour accomplir leurs tâches.

Accès et permissions temporaires pour les actions critiques

Au sein de Nuabee, nous avons instauré une procédure spécifique pour la gestion des accès temporaires aux ressources Cloud, en particulier pour les actions critiques. Cette approche vise à réduire les risques d'accès non autorisé ainsi que les dangers liés à l'exécution de tâches sensibles, telles que la suppression de données sensibles ou la modification des configurations de sécurité.

- **Gestion des Accès Temporaires** :
  - Pour les actions particulièrement sensibles ou à haut risque, nous attribuons des permissions temporaires aux collaborateurs. Ces permissions sont accordées pour une durée limitée et sont conçues pour permettre l'exécution précise de tâches sensibles tout en minimisant les risques associés. Les utilisation des ressources est de toute façon enregistrée dans le système de gestion des logs et des traces du Cloud

- **Flexibilité et Sécurité** :
  - Cette méthode nous permet de maintenir un contrôle strict sur les opérations critiques tout en offrant la flexibilité nécessaire pour gérer les interventions urgentes ou les maintenances planifiées. En limitant les permissions dans le temps, nous assurons que les droits d'accès ne restent actifs que pendant la durée nécessaire à la réalisation de la tâche, réduisant ainsi les risques potentiels.

- **Protection des Environnements Cloud** :
  - En mettant en place ces mesures, nous garantissons la sécurité et l'intégrité des environnements Cloud. Cette procédure rigoureuse assure non seulement la protection des données sensibles mais aussi le respect des normes élevées en matière de gestion des accès. Ainsi, nous veillons à ce que chaque opération critique soit effectuée dans un cadre sécurisé et contrôlé.

Conclusion

La gestion des identités et des accès (IAM) est essentielle pour assurer la sécurité des environnements Cloud. En utilisant des permissions finement ajustées et en mettant en œuvre des processus d'accès temporaires pour les actions critiques, nous renforçons la sécurité tout en

offrant la flexibilité nécessaire pour gérer efficacement les tâches sensibles.

Ces pratiques permettent de protéger les données et les ressources, tout en respectant des standards rigoureux en matière de gestion des accès. En appliquant ces principes, nous nous assurons que les environnements Cloud reste sécurisée et conforme aux meilleures pratiques de l’industrie.

Pour aller plus loin : documentation sur la gestion des identités et des accès