Les solutions de sécurité Cloud dans les espaces de PRA

Architecture sécurité · https://preview.nuabee.fr/documents/solutions-securite-cloud-espaces-pra/

Introduction

Dans un espace de PRA Client, la sécurité est une priorité absolue pour protéger les ressources informatiques. Cet article présente les solutions de sécurité natives disponibles dans le cloud T Cloud Public (anciennement Open Telekom Cloud), offrant des fonctionnalités robustes pour la protection des ressources.

Nous explorerons en détail les groupes de sécurité, les listes de contrôle d'accès (ACL), la gestion des identités et des accès (IAM), les systèmes de surveillance comme CloudEye, les logs CloudTraceService (CTS), l'isolation des réseaux privés virtuels (VPC), et les options de connexion sécurisée comme le VPN IPSec.

Les solutions de sécurité Cloud de T Cloud Public

Groupes de Sécurité

Les **groupes de sécurité** agissent comme des pare-feu virtuels qui contrôlent le trafic réseau à destination et en provenance des instances. Ces groupes permettent de définir des règles de trafic basées sur des critères spécifiques :

- **Règles d'entrée et de sortie** : Les règles d'entrée spécifient le trafic autorisé à entrer dans une instance, tandis que les règles de sortie contrôlent le trafic sortant. Par exemple, une règle d'entrée peut autoriser uniquement le trafic HTTP (port 80) et HTTPS (port 443) à partir de certaines adresses IP.
- **Filtrage par IP et port** : Les administrateurs peuvent restreindre l'accès à certaines plages d'adresses IP ou à des ports spécifiques, ce qui permet de limiter les points d'entrée potentiels aux seules adresses ou services nécessaires.

- **Stateless vs Stateful** : Les groupes de sécurité sont généralement stateful, ce qui signifie que les réponses au trafic autorisé sont automatiquement autorisées, simplifiant ainsi la gestion des règles.

Listes de Contrôle d'Accès (ACL)

Les **listes de contrôle d'accès (ACL)** fournissent un contrôle du trafic réseau au niveau des sous-réseaux, offrant une granularité supplémentaire dans la gestion de la sécurité :

- **Règles de contrôle du trafic** : Les ACL permettent de définir des règles qui acceptent ou refusent le trafic basé sur des critères comme l'adresse IP source, l'adresse IP de destination, les ports et les protocoles.
- **Filtrage avancé** : Contrairement aux groupes de sécurité, les ACL peuvent s'appliquer à des niveaux de réseau plus spécifiques, comme le contrôle du trafic entre sous-réseaux ou même entre interfaces réseau individuelles.
- **Ordre des règles** : Les ACL sont généralement évaluées dans un ordre spécifique, ce qui signifie que la première règle correspondante est appliquée. Une gestion prudente de l'ordre des règles est donc cruciale pour une sécurité efficace.

Gestion des Identités et des Accès (IAM)

La **gestion des identités et des accès (IAM)** est essentielle pour gérer les utilisateurs et les permissions :

- **Utilisateurs, groupes et rôles** : IAM permet la création d'entités utilisateurs et groupes, et l'attribution de rôles avec des permissions spécifiques. Par exemple, un rôle peut permettre l'accès en lecture à certaines ressources, mais interdire les modifications.
- **Politiques basées sur les rôles** : Les politiques IAM définissent les actions que les utilisateurs ou rôles peuvent effectuer, comme la gestion des ressources ou l'accès aux services spécifiques.
- **Multi-factor Authentication (MFA)** : L'implémentation de l'authentification multi-facteurs renforce la sécurité des comptes en exigeant une deuxième forme d'identification, comme un code SMS ou une application d'authentification.

Plus de détail

Solution de surveillance CloudEye

CloudEye est une solution de surveillance qui offre une visibilité complète sur les ressources du cloud :

- **Surveillance des ressources** : CloudEye permet de surveiller des métriques clés comme l'utilisation du CPU, la mémoire, et les E/S disque, ainsi que des indicateurs réseau.
- **Alertes personnalisées** : Les administrateurs peuvent configurer des alertes basées sur des seuils spécifiques.
- **Intégration avec d'autres services** : CloudEye peut être intégré avec des systèmes de gestion des incidents pour automatiser les réponses aux alertes, améliorant ainsi la résilience opérationnelle.

Plus de détail

CloudTraceService (CTS)

CloudTraceService est un service de journalisation qui enregistre les actions et les événements dans le cloud :

- **Audit des actions utilisateur** : Enregistre les activités des utilisateurs, comme la création de ressources, les modifications de configuration, ou les tentatives d'accès échouées.
- **Traçabilité des modifications** : Suivi des modifications apportées aux ressources et aux configurations, ce qui est crucial pour le diagnostic des incidents et la conformité.
- **Analyse des incidents** : Les journaux détaillés permettent d'analyser les événements passés pour identifier les causes profondes des problèmes de sécurité.

Plus de détail

Isolation des VPC

L'**isolation des Virtual Private Clouds (VPC)** assure que les ressources d'un VPC ne sont pas accessibles directement depuis un autre VPC :

- **Segments de réseau isolés** : Chaque VPC est un environnement réseau isolé, permettant aux entreprises de séparer les environnements de production, de développement et de test.
- **Contrôles de routage** : Les règles de routage et les tables de routage permettent de contrôler le trafic entre différents VPC ou sous-réseaux, renforçant l'isolation.

- **Peering de VPC** : Permet la connexion privée entre deux VPC, tout en maintenant l’isolation des autres ressources, idéal pour les scénarios de multi-environnement.

Conclusion

Les solutions de sécurité natives dans le cloud fournissent une base solide pour protéger les données et les applications. En combinant des outils tels que les groupes de sécurité, les ACL, IAM, CloudEye, CloudTraceService, l’isolation des VPC, et VPN IPSec, nous avons la capacité de construire un espace de PRA résiliente et conforme.

Ces outils nous permettent de prévenir les menaces, d’assurer la conformité aux régulations, et de répondre rapidement aux incidents de sécurité, garantissant ainsi la continuité des opérations et la protection des actifs numériques.