Architecture sécurité de la solution Nuabee

Architecture sécurité · https://preview.nuabee.fr/documents/architecture-securite-solution-nuabee/

Introduction

Nuabee offre une solution complète de sauvegarde et de Plan de Reprise d'Activité (PRA), conçue pour garantir la confidentialité, l'intégrité et la disponibilité des sauvegardes tout au long de leur cycle de vie. Voici un aperçu détaillé de l'architecture sécurisée de la solution Nuabee, mettant en lumière les différentes étapes de la protection des données, du chiffrement initial des sauvegardes à la gestion des clés de chiffrement.

Sauvegardes chiffrées à la source

La sécurité des données chez Nuabee commence dès la création des sauvegardes. Toutes les données sont chiffrées à la source, c'est-à-dire avant même qu'elles ne quittent l'infrastructure du client. C'est de la responsabilité du Client de définir la clef de chiffrement des sauvegardes et de la stocker dans un endroit sécurisé.

Ce processus de chiffrement initial utilise des algorithmes de chiffrement avancés (AES) pour garantir que les données sont protégées contre les accès non autorisés dès leur origine. En chiffrant les données à la source, Nuabee assure une première ligne de défense robuste contre les tentatives de compromission.

Transport sécurisé des sauvegardes vers le Cloud

Une fois chiffrées, les sauvegardes sont transportées vers le cloud de manière sécurisée. Nuabee utilise des protocoles de transmission sécurisés pour protéger les données en transit. Ces protocoles incluent des technologies telles que SSL/TLS, qui assurent que les données ne peuvent être interceptées ou modifiées lors de leur transfert vers les environnements Cloud.

Ce transport sécurisé est crucial pour maintenir l'intégrité et la confidentialité des données pendant leur acheminement.

Stockage sécurisé dans le Cloud

Les sauvegardes chiffrées sont conservées dans un environnement Cloud isolé et hautement sécurisé.

Plus précisément, elles sont stockées dans des buckets dédiés S3, un service de stockage d'objets réputé pour sa flexibilité et sa sécurité. Le stockage objet S3 fournit des fonctionnalités avancées pour garantir la durabilité, la disponibilité et la protection des données.

Nuabee met en œuvre des configurations rigoureuses pour le stockage S3 afin d'assurer que les données sont protégées par des mesures de sécurité robustes, telles que le chiffrement des données au repos et des contrôles d'accès granulaires. Conçu pour une haute durabilité, S3 utilise une architecture de redondance des données pour assurer une disponibilité continue. De plus, les buckets S3 permettent une gestion fine des accès et des permissions, offrant un contrôle précis sur les personnes autorisées à consulter ou modifier les données stockées.

En complément de ces mesures, Nuabee a mis en place un processus sécurisé en interne pour gérer les modifications critiques des données stockées dans ces buckets. Ce processus est activé à la suite de demandes spécifiques des clients, et implique des vérifications rigoureuses pour assurer que seules les personnes autorisées peuvent effectuer des modifications sur le stockage. Les modifications critiques, telles que la restauration ou la suppression de données, sont strictement contrôlées et auditées pour garantir la sécurité et l'intégrité des données.

Immutabilité des sauvegardes dans S3

Nuabee offre la possibilité de stocker les sauvegardes dans des buckets S3 avec une fonctionnalité d'immutabilité. L'immutabilité des données garantit que les sauvegardes ne peuvent pas être modifiées ou supprimées pendant une période déterminée. Cette fonctionnalité est activée en utilisant l'option Object Lock, qui ajoute une couche supplémentaire de sécurité en rendant les données inaltérables pour une durée définie.

Gestion sécurisée des clés de chiffrement

Les clés de chiffrement utilisées pour chiffrer les sauvegardes à la source sont gérées avec le plus haut niveau de sécurité. Elles sont stockées dans un coffre-fort numérique, chiffrées, et totalement inaccessibles aux humains. Ce coffre-fort est conçu pour protéger les clés de toute tentative d'accès non autorisé, en assurant que seules les procédures automatisées d'industries, appelées « indus », peuvent les utiliser.

Cette indus est la seul à pouvoir accéder aux clés de chiffrement, et uniquement pour des processus spécifiques tels que la restauration des données lors des PRA ou des tests de PRA. Cette approche garantit que même en cas de compromission du système, les clés de chiffrement restent protégées et les données sécurisées.

Gestion des Identités et des Accès (IAM) dans les espaces de PRA

Dans les environnements de Plan de Reprise d'Activité (PRA) de Nuabee, la gestion des identités et des accès (IAM) est essentielle pour garantir la sécurité des données critiques. Nuabee applique des contrôles d'accès granulaire, s'assurant que seuls les utilisateurs autorisés peuvent accéder et manipuler les ressources nécessaires. L'authentification multifacteurs (MFA) aux environnements Cloud renforce cette sécurité en ajoutant une couche de vérification supplémentaire.

Les accès sont rigoureusement surveillés et enregistrés, avec des journaux d'activité régulièrement audités pour détecter toute anomalie. De plus, des processus stricts sont en place pour gérer les accès temporaires en cas d'intervention d'urgence, garantissant que chaque opération est effectuée en toute sécurité et conformément aux politiques de sécurité.

Plus de détail

Solutions de sécurité natives au Cloud T Cloud Public

Pour renforcer la protection des données et des ressources, Nuabee intègre des solutions de sécurité natives au cloud telles que Cloud Trace Service (CTS) et CloudEye.

Cloud Trace Service (CTS) fournit une surveillance détaillée des activités dans l'environnement cloud, en enregistrant les événements pour une visibilité complète sur les actions effectuées et les accès aux ressources. Cela permet de détecter et d'analyser les comportements suspects ou non conformes, offrant ainsi une réponse rapide aux incidents potentiels.

CloudEye, quant à lui, est une solution de surveillance et d'alerte en temps réel qui surveille l'état et la performance des ressources cloud. Il fournit des alertes proactives sur les anomalies et les menaces potentielles, permettant une gestion efficace des incidents avant qu'ils n'affectent les opérations. En combinant ces outils de sécurité, Nuabee assure une

protection renforcée contre les menaces internes et externes, tout en offrant une visibilité complète et une réponse rapide aux incidents de sécurité dans les environnements cloud.

En complément, Nuabee utilise des **Security Groups** et des **Listes de Contrôle d'Accès (ACL)** pour contrôler le trafic réseau et sécuriser les instances cloud. Les Security Groups agissent comme des pares-feux virtuels, définissant des règles d'entrée et de sortie pour les instances, tandis que les ACL offrent un contrôle plus granulaire sur le trafic réseau au niveau des sous-réseaux.

L'**isolation des VPC (Virtual Private Cloud)** est également une composante clé, permettant de segmenter le réseau pour isoler les différentes applications et données, minimisant ainsi les risques de compromission latérale en cas de violation de sécurité.

Conclusion

L'architecture sécurisée de la solution Nuabee offre une protection de bout en bout pour les données des clients, du chiffrement initial à la gestion des clés. En chiffrant les données à la source, en assurant un transport sécurisé vers le cloud, et en offrant des options d'immutabilité, Nuabee les protège efficacement contre les menaces internes et externes.

La gestion rigoureuse des clés de chiffrement, avec un accès limité aux indus pour les opérations de restauration, assure que la sécurité des données est maintenue à chaque étape. Grâce à ces mesures, Nuabee fournit une solution de sauvegarde et de PRA répondant aux exigences de sécurité et de fiabilité du marché.