La gestion des secrets via le Vault Nuabee

Architecture sécurité · https://preview.nuabee.fr/documents/gestion-des-secrets-via-un-vault/

Le choix du Vault HashiCorp chez Nuabee

Le Vault est une technologie de gestion sécurisée des secrets développée par HashiCorp. Cette technologie Vault permet de stocker de manière chiffrée différents types de secrets comme, par exemple :

- Clé de chiffrement
- Identifiants de connexion

Les principes du Vault HashiCorp

Processus de scellement (Seal)

Le scellement dans le Vault fait référence au processus de chiffrement et de verrouillage des données sensibles stockées dans le système.

Lorsque le Vault est « scellé » :

- Toutes les données sont chiffrées et inaccessibles
- Les clés de déchiffrement sont supprimées de la mémoire
- Aucune opération de lecture ou d’écriture ne peut être effectuée

Ce mécanisme assure que les informations sensibles restent protégées, même si un attaquant obtient un accès physique au serveur Vault.

Processus de descellement (Unseal)

Le descellement est le processus inverse, qui consiste à déverrouiller le Vault et le rendre opérationnel :

- Il nécessite généralement plusieurs clés partielles (appelées « key shares »).
- Ces clés sont combinées pour reconstruire la clé principale de déchiffrement.
- Une fois déverrouillé, le Vault peut accéder et gérer les secrets stockés.

Ce processus de descellement ajoute une couche de sécurité supplémentaire, car il requiert la participation de plusieurs « entités » détenant chacune une partie de la clé.

L'utilisation du « seal » et « unseal » dans Vault permet de maintenir un niveau élevé de sécurité pour les données sensibles, tout en offrant un mécanisme contrôlé pour accéder à ces informations lorsque nécessaire.

Durcissement du Vault

Nous avons réalisé des analyses de risques afin de mettre en place un durcissement du Vault.

Fragmentation des clés

Le scénario de risque étudié est le suivant : vol du token d'authentification.
Ceci permettrait à l'attaquant d'appeler les API et utiliser notre système de chiffrement/déchiffrement et stockage/récupération des mots de passe des clients.

Nuabee utilise l'algorithme connu sous le nom de « Shamir's Secret Sharing » pour diviser une clé en plusieurs fragments. Un certain seuil de fragments est nécessaire pour reconstruire cette clé de chiffrement, qui est ensuite utilisée pour déchiffrer la clé « Master ».

- **Le processus de descellement** : les fragments sont ajoutés un à la fois (dans n'importe quel ordre) jusqu'à ce qu'il y ait suffisamment de fragments pour reconstruire la clé de chiffrement et décrypter la clé « Master ».
- **Le processus de scellement** : la clé de chiffrement combinée à l'aide de l'algorithme « Shamir's Secret Sharing » est utilisée pour chiffrer la clé « Master ».

Plus précisément, les fragments seront distribués sur plusieurs environnements Cloud dans plusieurs pays. Quand il est nécessaire, des tâches seront attribuées à chacun des serveurs afin qu'ils « unseal » le Vault durant un intervalle de temps suffisant pour restaurer les mots de passe.

Cette solution permet d**e ne pas rendre accessible les mots de passe par des humains**, aucun administrateur de la solution ne peut connaître les mots de passe, uniquement le système d'industrialisation Nuabee a la capacité de le récupérer en clair au travers ces mécanismes de sécurisation.

Enveloppe de chiffrement

Pour évaluer les conséquences d'une intrusion, on peut élaborer des arbres d'attaque. Cette méthode, applicable aux systèmes industriels, permet d'identifier les différentes étapes

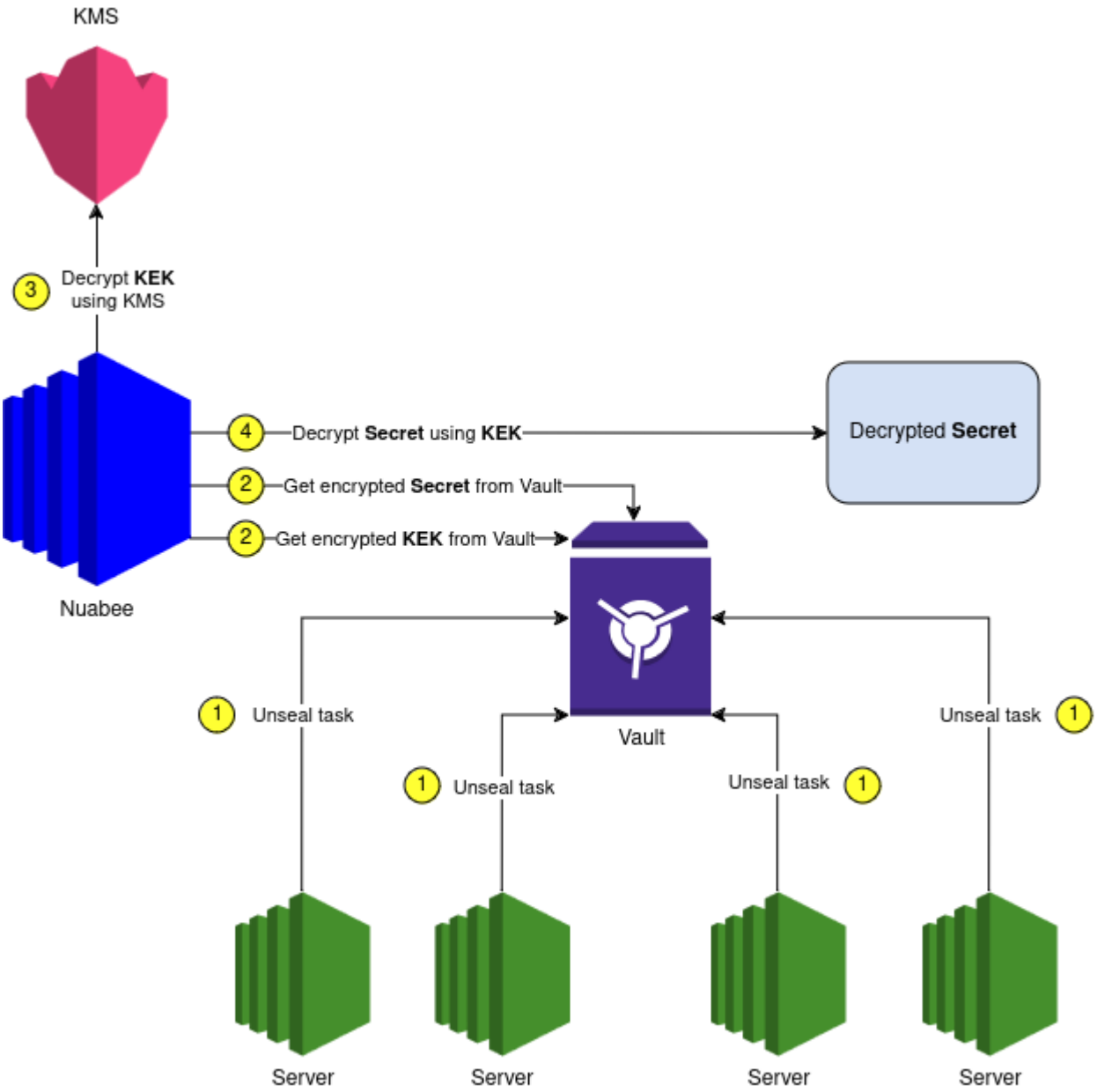
nécessaires à l'attaque d'un système, et de visualiser les conséquences de sa compromission. On peut alors prendre des mesures préventives pour protéger les parties les plus critiques de l'infrastructure.

Pour qu'un attaquant puisse extraire les mots de passe des clients, il faudrait exploiter le serveur Vault. Plusieurs scénarios sont envisageables menant vers une exploitation pareille : Vault zero-day vulnerability, niveau de patch non récent, vol de tokens, vol des fragments permettant de reconstruire la clé de chiffrement…

Afin de sécuriser au mieux les secrets enregistrés dans ce Vault, Nuabee a mis en place un chiffrement par « Enveloppe ». Etant hébergés dans des Clouds de confiance tel que T Cloud Public, Nuabee opère un chiffrement à l'aide du système KMS (Key Management System) du Cloud et ensuite stocke le résultat du chiffrement dans le Vault. Le chiffrement d'enveloppe repose sur :

- Le chiffrement d'enveloppe est une procédure qui consiste à chiffrer des données avec une clé DEK (Data Encryption Key) et ensuite chiffrer cette clé DEK à l'aide d'une clé KEK (Key Encryption Key).
- Nuabee sécurise les secrets de ses clients grâce à une CMK, une clé de chiffrement KEK (Key Encryption Key), créée par un utilisateur à l'aide du KMS cloud T Cloud Public.

En conséquence, un attaquant devrait non seulement exploiter le serveur Vault pour extraire les mots de passe mais aussi exploiter le système KMS du cloud T Cloud Publi, ce qui permet d'approfondir l'arbre d'attaque.



Descriptions des 4 étapes de déchiffrement

1. Les tâches de « unseal » permettent de déverrouiller le Vault grâce à plusieurs clés de déchiffrement distribuées sur différents serveurs.
2. Depuis le Vault, on récupère la KEK (Key Encryption Key), qui est chiffrée par le KMS, ainsi que le secret, chiffré par la KEK.
3. Déchiffrement de la KEK avec le KMS.
4. En utilisant la KEK déchiffrée à l’étape 3, on déchiffre le secret pour obtenir sa version en clair.

En conclusion

Nous avons mis en œuvre les meilleures pratiques de sécurité pour assurer le fonctionnement des Plans de Reprise d'Activité de nos Clients, tout en s'appuyant sur nos partenaires Cloud de confiance tels que T Cloud Public et OVH.

Le Vault de HashiCorp est ainsi une solution très sécurisée de protection des secrets grâce à plusieurs fonctionnalités techniques avancées :

- **Chiffrement robuste** : Utilisation du chiffrement AES-256 pour protéger les données au repos et en transit.
- **Authentification multi-facteurs** : Soutient diverses méthodes d'authentification, y compris les certificats TLS, les jetons JWT, et l'authentification basée sur les rôles.
- **Contrôle d'accès basé sur les rôles (RBAC)** : Utilise des politiques pour contrôler l'accès aux secrets en fonction des rôles et des responsabilités.
- **Architecture distribuée** : Conçu pour une haute disponibilité, réduisant les risques de perte de données et assurant la continuité des services.
- **Gestion dynamique des secrets** : Les secrets sont générés dynamiquement et révoqués rapidement en cas de compromission.
- **Audit et traçabilité** : Les accès sont tracés pour garantir la responsabilité et la sécurité des opérations, facilitant la conformité réglementaire.
- **Protection contre les attaques par force brute** : Utilise des mécanismes pour limiter les tentatives d'authentification incorrectes.
- **Conformité réglementaire** : Conforme à divers standards de sécurité, tels que PCI-DSS et HIPAA, pour assurer la conformité réglementaire.